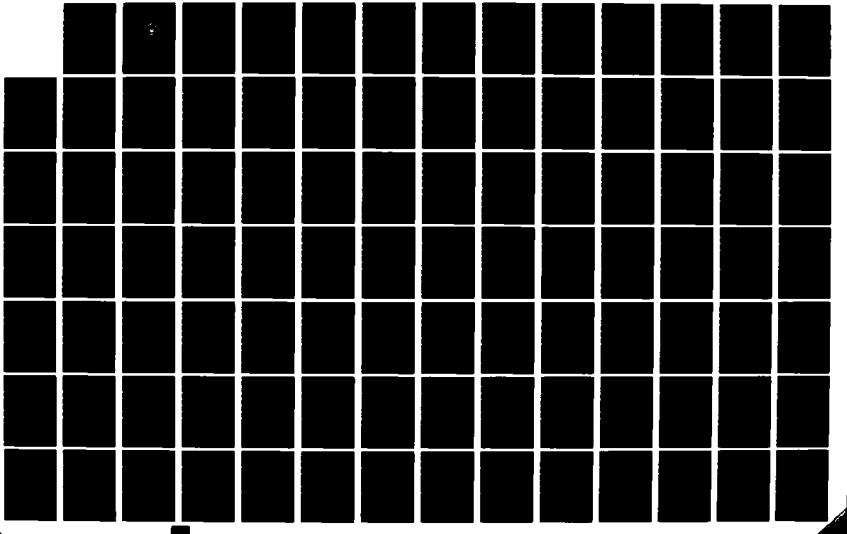
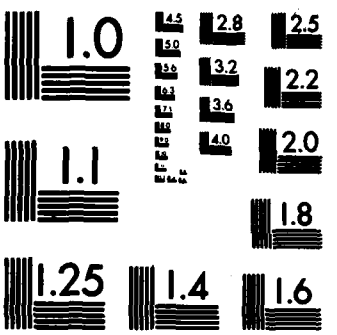
AD-A127 244 A GUIDE FOR DEVELOPING AN ADP SECURITY PLAN FOR NAVY FINANCE CENTER CLEVELAND OHIO(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA D E BARBER ET AL. DEC 82 1/3

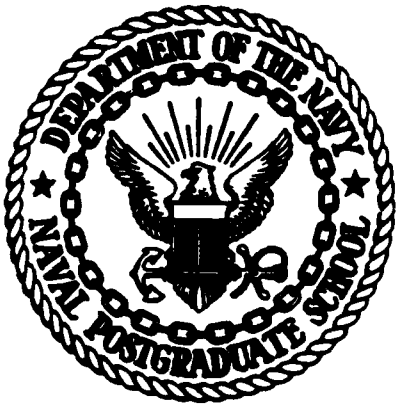
UNCLASSIFIED F/G 9/2 NL





(2)

NAVAL POSTGRADUATE SCHOOL
Monterey, California



THESIS

A GUIDE FOR DEVELOPING AN ADP SECURITY PLAN FOR NAVY FINANCE CENTER, CLEVELAND, OHIO

by

Daniel E. Barber
Elwood Thomas Hodnett, Jr.

December 1982

Co-advisor: Dan C. Boger
Co-advisor: Norman F. Schneidewind

Approved for public release; distribution unlimited

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. A127844	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) A Guide for Developing an ADP Security Plan for Navy Finance Center, Cleveland, Ohio		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis December 1982 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Daniel E. Barber Elwood Thomas Hodnett, Jr.		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		12. REPORT DATE December 1982 13. NUMBER OF PAGES 232
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Automatic Data Processing (ADP)
Security
Computer
Contingency Plan
Risk Analysis
Management
Auditing

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This paper is intended to be used as a guide by personnel at the Navy Finance Center (NFC), Cleveland, Ohio in developing an Automatic Data Processing (ADP) Security Plan. An effort has been made to combine the requirements for an ADP security plan established by OPNAVINST 5239.1A with pertinent information from other selected readings.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

The importance of the devotion of personnel, time and funds to ADP security planning has been emphasized. Individual chapters have been devoted to the elements that must be considered when developing an ADP security plan. They include risk assessment, physical security, systems security, contingency planning and the managerial procedures necessary for the implementation of an ADP security plan.

This paper, used in conjunction with OPNAVINST 5239.1A, should provide ample guidance for the development of an initial ADP security plan for NFC, Cleveland.

Approved for public release; distribution unlimited

A Guide for Developing an ADP Security Plan for Navy Finance Center, Cleveland, Ohio

by

Daniel E. Barber
Captain, United States Marine Corps
B.B., Western Illinois University, 1971

Elwood Thomas Hodnett, Jr.
Lieutenant Commander, Supply Corps, United States Navy
B.S., Virginia Polytechnic Institute & State University, 1972

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 1982

Author: Daniel E. Barber

Author: Elwood Thomas Hodnett Jr.

Approved by: Dan C. Boger
Co-advisor

Norman F. Schneidewind
Co-advisor

Chairman, Department of Administrative Sciences

Dean of Information and Policy Sciences

ABSTRACT

This paper is intended to be used as a guide by personnel at the Navy Finance Center (NFC), Cleveland, Ohio in developing an Automatic Data Processing (ADP) Security Plan. An effort has been made to combine the requirements for an ADP security plan established by OPNAVINST 5239.1A with pertinent information from other selected readings.

The importance of the devotion of personnel, time and funds to ADP security planning has been emphasized. Individual chapters have been devoted to the elements that must be considered when developing an ADP security plan. They include risk assessment, physical security, systems security, contingency planning and the managerial procedures necessary for the implementation of an ADP security plan.

This paper, used in conjunction with OPNAVINST 5239.1A, should provide ample guidance for the development of an initial ADP security plan for NFC, Cleveland.

TABLE OF CONTENTS

I. BACKGROUND AND PURPOSE

The purpose of this paper is to provide a guide that will assist the staff of the Navy Finance Center (NFC) in Cleveland, Ohio with the preparation of a realistic automatic data processing (ADP) security plan. The requirement for the development of an ADP security plan by all Department of the Navy sponsored ADP activities will be explained. The need for a workable ADP security plan will become evident as the Navy's personnel and pay (PERSPAY) phasing plan is detailed.

The Deputy Chief of Naval Operations (Manpower, Personnel and Training)/Navy Comptroller (DCNO(MP&T)/NAVCOMPT) Brand X Site Study was conducted collectively by representatives of the Bureau of Naval Personnel, Navy Finance Center and Naval Data Automation Command. Its results were published on 15 February 1979. "The purpose of this study was to conduct an economic analysis of four alternatives for the site selection of the 'Brand X' computer equipment for the Navy Finance Center (NAVFINCEN), Cleveland, Ohio and the Bureau of Naval Personnel (BUPERS), Washington, D.C. Work began in May 1978 with completion scheduled for July 1978 then rescheduled for January 1979" [Ref. 1: p. 1-1].

Why was the Brand X study conducted?

> Both BUPERS and NAVFINCEN are receiving computer support from computer centers with hardware authorized by interim delegation of procurement authority (DPA) from the General

> Services Administration (GSA). The BUPERS interim DPA expires in April 1979 and the NAVFINCEN interim DPA expires in January 1979. In July 1978, an extended DPA was granted for continued use of the BUPERS 370/165 computer and NAVFINCEN's IBM dual 370/158 computer system through February 1982. BUPERS and NAVFINCEN have been directed by GSA to replace their present computer systems through the competitive procurement process. BUPERS and NAVFINCEN will procure these replacements through a single joint effort, which will be referred to as the "Brand X" computer procurement. The determination of the ultimate site/sites of the "Brand X" computer equipment will be the purpose of this economic analysis. [Ref. 1: p. 1-2]

When the results of the Brand X study were published on 15 February 1979, the recommendation was that the BUPERS and NAVFINCEN Brand X computers be co-located at the Navy Finance Center (Bratenaal Annex) in Cleveland, Ohio [Ref. 1: p. 1-4].

"In March 1978 the Navy initiated the PERSPAY project to to combine the ADP procurement offorts of DCNO(MP&T) and NAVCOMPT" [Ref. 2: p. 1]. The primary purpose of the PERSPAY project is to lower costs by initiating one instead of two separate competitive procurements and to provide a formal management discipline by employing the Commander, Naval Data Automation Command (NAVDAC) as the project manager. For the purpose of this paper, the PERSPAY project is best viewed as an opportunity to facilitate the interface of pay and personnel information systems [Ref. 2: p. 2].

The culmination of efforts to join pay and personnel systems will be the dedication of a consolidated data center in Cleveland, Ohio during March, 1987, but the phasing-in process of this major merger is already underway.

Large volumes of information have become easier to store as computer technology has been improved. As people have become more familiar with computers, the information stored in the computer has become more easily accessible to more people. The advent of remote terminals has made information stored in computers more readily accessible to more people than ever before. The purpose of this paper now becomes clear. Information that used to be locked in a file cabinet, in a locked office with a guard at the main entrance of the building, was considered secure. Unless there were signs of forced entry, you could be reasonably certain that the information in the locked file cabinet had not been compromised in your absence. Much of the same information that used to be stored in the locked file cabinet is now stored in computers. With remote computer terminals being readily accessible, can the same feeling of security be maintained about the information stored in the computer as there was when it was stored in a file cabinet? Obviously not. Information security is no longer a simple matter of locking papers in a drawer.

A security plan is needed at NFC Cleveland because of the type of data that is stored in their ADP facility. As we can best determine, the information that is presently stored in the computer at NFC Cleveland and the information that will be stored in the computer when the consolidated data center evolves will be information protected by the "Privacy Act of

1974." More specifically, the "Privacy Act of 1974" states the following:

(a) The Congress finds that:

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to:

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records,

to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act. [Ref. 3: p. 1]

The Commanding Officer or any person associated with ADP may, now, be held more directly responsible for his actions. It means that the Commanding Officer and any other person that works at the data center can be subject to a civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under the "Privacy Act of 1974." This means that the Commanding Officer can be held financially liable from his personal funds for improper actions by himself concerning Privacy Act information. Military and civilian government employees have had to spend personal funds because of improper action concerning computer security.

As could be expected in any area with such possible far-reaching impact as computer security, the Department of the

Navy (DON) has issued OPNAVINST 5239.1A dated 3 August 1982 that requires all DON automatic data processing (ADP) activities to submit a copy of their activity ADP security plan (AADPSP) to the Commander, Naval Data Automation Command (COMNAVDAC) for approval within nine months of the date of this instruction [Ref. 4: p. 3]. The objectives of the instructions are much farther reaching than merely imposing a requirement on all DON ADP activities. The stated objectives are to:

a. Provide centralized guidance and uniform policy on all known and recognized aspects of ADP security.

b. Provide a graduate program of ADP security which is responsive to the security requirements and needs of ADP systems and networks commensurate with their data sensitivity and mission criticality.

c. Provide for operational reliability and asset integrity for all ADP systems and networks.

d. Provide realistic guidance and generalized procedures to ensure that all data handled by ADP activities and networks are adequately protected against accidental or intentional destruction, modification, and disclosure, and users are protected against denial of service which may result from events such as fraud, misuse, espionage, sabotage, malicious acts, natural hazards, or fire. [Ref. 4: p. 2-3]

The fact that the instruction exists and imposes a requirement for an activity ADP security plan (AADPSP) shows us that the Navy recognizes the seriousness of the situation. The value of this instruction is increased drastically because it describes "how to" develop each part of a total activity ADP security program. It is stated in the instruction that an AADPSP should address the following areas:

(1) Scope of the activity ADP security program.

(2) Commanding Officer's policy statement.

(3) ADP security organization and assignment of responsibilities.

(4) Objectives for implementing the DON ADP security program at the activity.

(5) Top level description of the current ADP security environment:

  (a) hardware;

  (b) software;

  (c) physical facility/security;

  (d) personnel;

  (e) emanations;

  (f) administrative/operating procedures.

(6) Training.

(7) Audit/internal review.

(8) Provisions for ADP security in life cycle management.

(9) Provisions for ADP security in hardware and software configuration control.

(10) Activity accreditation schedule identifying all ADP elements and a plan of action and milestones (POA&M) for completing the following:

  (a) Risk assessments;

  (b) Security tests and evaluations (ST&Es);

  (c) Contingency planning and testings;

  (d) Accreditations.

Updating the AADPSP should be a principle of the execution of the plan. The AADPSP should be a living document for baselining, updating, improving, developing, maintaining, and managing ADP security requirements within the DON ADP activity. The AADPSP should serve as a comprehensive

document of security posture and plans for the Commanding Officer and ADPSO. The ADPSO is responsible for developing, implementing, and updating the AADPSP. [Ref. 4: pp. H-1 - H-2]

Although OPNAVINST 5239.1A imposes the requirement for an AADPSP and gives good guidance on how to develop the plan, it is the purpose of this paper to amplify the most important areas of OPNAVINST 5239.1A while introducing some areas that are not mentioned in OPNAVINST 5239.1A and should possibly be included in NFC's AADPSP. It is intended that this paper be used as a working tool to help NFC personnel develop an AADPSP that not only satisfies OPNAVINST 5239.1A requirements but will be a legitimately useful document for ensuring and safeguarding the efficient running of the NFC.

Before the section on plan development is begun, a few additional comments about OPNAVINST 5239.1A and the specific situation at the NFC are appropriate. It should be understood that an AADPSP that is developed for the current situation at the NFC will have to be under a continuous review and modification as the facility changes and it gets closer to the dedication date for the consolidated data center. This does not mean that less effort should be put into the initial draft of the AADPSP. A good initial AADPSP will serve as a sound base from which to improve the security posture.

OPNAVINST 5239.1A addresses the subject of an activity ADP security staff. From our research we have ascertained that most Navy ADP facilities do not have a formal security

staff as described in OPNAVINST 5239.1A. In most cases ADP security has been assigned as a less important collateral duty to one or at most two persons. It is understood that the assignment of ADP security staff duties to the present staff at most commands without additional personnel would cause an undue hardship on personnel and possibly endanger the command's mission. It is therefore recommended that duties be assigned to current personnel only until permanent positions can be requested, approved and filled. The initial personnel assigned to the ADP security staff must move forward in the development of an AADPSP and therefore it is recommended that members of this staff be carefully reviewed and selected from all volunteers. The implementation of a viable ADP security plan will require significant increases in staff, time and money.

The remainder of this paper will be devoted to the amplification of subjects on how to best develop and implement an AADPSP. The following subject areas will be addressed: development of a plan of action and milestones (POA&M); types of ADP security; risk assessment; physical security; managerial procedures; systems security; contingency plan development; procedures for handling security violations; ADP security training plan development; and how to prepare for an ADP security audit.

II. SECURITY STAFF ORGANIZATION AND THE DEVELOPMENT OF A PLAN OF ACTION AND MILESTONES (POAM)

A. INITIAL ORGANIZATION

The first step in the development of an ADP security plan will be the organization of an ADP security staff. While conducting research for this paper, it was noted that the majority of governmental ADP organizations in which we made contact do not have formal staffs devoted to ADP security. In most cases, the responsibility had been delegated to one person as a collateral duty. Most command representatives interviewed recognized the need for a full time ADP security staff but, because of manning allowances, the movement has been slow. The advent of OPNAVINST 5239.1A has imposed the requirement for an ADP security staff and defined each member's responsibility. The existence of OPNAVINST 5239.1A should provide the much-needed formal justification for commands to obtain the manning for a proper ADP security staff. The implementation of a proper ADP security staff may not happen immediately, but should be phased in during the near future.

B. TYPES OF DATA

The responsibilities of the Commanding Officer must initially be defined when organizing an ADP security staff, and

the type of data to be protected must be determined because the Commanding Officer's responsibilities will vary depending on the type of data to be safeguarded. At NFC Cleveland, it has been determined that the highest data type of information to be safeguarded will be Level II as defined by OPNAVINST 5239.1A. The definitions of the different levels of data classification are as follows:

Level I. Classified data;

Level II. Unclassified data requiring special protection, e.g., Privacy Act, For Official Use Only, etc.;

Level III. All other unclassified data. [Ref. 4: p. 1-2]

C. RESPONSIBILITIES OF THE COMMANDING OFFICER

When the type of data to be protected has been properly classified into the appropriate level, the responsibilities of the Commanding Officer can be defined. The Commanding Officer of NFC Cleveland, where Level II data will be the most highly classified data, will be the Designated Approving Authority (DAA) for the accreditation of his ADP facility. As DAA for NFC Cleveland, the Commanding Officer's responsibilities will be as follows:

1. Develop an AADPSP and submit it to COMNAVDAC for approval (see Appendix H of Ref. 4);
2. Conduct a risk assessment (see Chapter 5 and Appendix E of Ref. 4);
3. Develop a Security Test and Evaluation (ST&E) Plan and conduct a ST&E (see Chapter 6 of Ref. 4);
4. Document the ST&E results (see Appendix H of Ref. 4);

5. Develop a contingency plan (see Chapter 7 of Ref. 4);

6. Prepare the accreditation support documentation (see Appendix H of Ref. 4);

7. Issue a Statement of Accreditation as described in paragraph 3.3C of Ref. 4;

8. Forward information copies of the accreditation support documentation and Statement of Accreditation to COMNAVDAC;

9. Provide logistic and administrative support to the ST&E test team as appropriate (if external from activity);

10. Fund technical assistance if local assistance is requested from COMNAVDAC. [Ref. 4: pp. 3-6 - 3-7]

The Commanding Officer, who is also the DAA for his activity, has the responsibility to declare his activity as either accredited or not accredited. He must declare one or the other. Accreditation is defined as the DAA's formal declaration that appropriate ADP security countermeasures have been properly implemented for the ADP activity. ADP activities not accredited may operate if the appropriate DAA has issued an interim authority to operate. Interim authority to operate is granted for a fixed period of time, generally a year, and is usually contingent upon certain conditions being met. Interim authority to operate is not a waiver of the requirement for accreditation. [Ref. 4: p. 3-1]

D. RESPONSIBILITIES OF STAFF MEMBERS

The importance of the Commanding Officer as an integral part in the development of a viable and successful ADP security plan cannot be overemphasized. A task that the

Commanding Officer should undertake as soon as possible is the organizing of a good ADP security staff, defining their responsibilities and establishing a Plan of Action and Milestones (POAM) for the implementation of a successful security plan. The positions that are recommended on an ADP security staff are as follows:

- ADP Security Officer (ADPSO);
- ADP Systems Security Officer (ADPSSO);
- Network Security Officer (NSO);
- Terminal Area Security Officer (TASO);
- Office Information System Security Officer (OISSO) [Ref. 4: p. A-2].

The responsibilities of the ADPSO, ADPSSO, NSO and TASO are clearly defined in Chapter 2 of OPNAVINST 5239.1A. Likewise, the responsibilities of the OISSO are defined in Chapter 4 of OPNAVINST 5239.1A and Chapter III of this thesis. It would normally be expected that there would be only one ADPSO and ADPSSO at each command. As the PERSPAY project becomes more fully developed and staffed, it may be necessary to provide assistants to the ADPSO and ADPSSO as required. The number of NSO's, TASO's and OISSO's will be dictated by the size of the operation, availability of personnel for assignment and the importance that the command places on ADP security. The command importance is reflected directly from the Commanding Officer. It is suggested that as many people as possible be aware of ADP security. This will facilitate

communication and training in ADP security areas while emphasizing the importance placed on ADP security by the Commanding Officer.

E. INITIAL STAFF MEETINGS

After the initial ADP security staff requirements have been made, an initial meeting of all staff members should be called. In this meeting, the Commanding Officer should communicate his opinions and priorities concerning ADP security while tasking the group to develop a feasible ADP security plan. The Commanding Officer should not be a normal participant at security staff meetings but should participate randomly at selected meetings in order to re-emphasize his opinions about ADP security and ensure the meetings are conducted in an appropriate manner. Communication of the Commanding Officer's seriousness about ADP security and a general awareness of basic steps that must be followed to ensure ADP security should be the initial assignment of the ADP security staff. The development of an ADP security plan in writing is only as good as it is communicated to the personnel that must implement the plan.

The first assignment of ADP security staff members, in addition to basic communication, should be for each of them to fill out the Security Checklist Assessment that is contained in Appendix A. This checklist is taken from OPNAVINST 5239.1A and will serve as a reference point from which the

second meeting can be developed. By filling out the checklist, it will cause the members of the security staff to become more familiar with ADP security at their own command. During the second meeting, which should be held as soon as practical, but allowing sufficient time for the Security Checklist Assessment to be properly reviewed, the results of the Security Checklist Assessment can be used for a basis to develop a Plan of Action and Milestones for the development of the ADP security plan. As the PERSPAY project is developed and the facility grows, a routine review of security using the checklist in Appendix A would keep the organization moving in the right direction. After the plan has been approved and the facility has received certification, the plan must be constantly reviewed to ensure that it continues to warrant accreditation. A review must be made at least every five years to verify that accreditation is still merited [Ref. 4: p. 5-1].

The results of the security checklist assessment in conjunction with the initial risk assessment as prescribed by OPNAVINST 5239.1A will serve as the basis for a realistic POAM in the development of the security plan. Before making assignments and establishing milestones, a careful review of the chapters discussing risk assessment, physical security, administrative security, system security and disaster recovery/contingency plan development would be appropriate.

The organization of a dedicated professional security staff with a realistic POAM is a necessary requirement. NFC Cleveland has the beginnings of a good security staff and the NFC Bratenahl Annex Security Manual discusses physical security and disaster recovery in some depth. With a little effort and time, NFC Cleveland could have an effective security staff and a viable security plan. The development of an efficient security plan that is constantly reviewed and updated must be the goal of NFC Cleveland.

III. TYPES OF SECURITY

A. OVERVIEW

Within the scope of this paper, two major topics pertaining to security will be discussed as being essential for an automatic data processing (ADP) security program at the Navy Finance Center. The first topic is referred to as computer security and includes the following major subtopics.

1. Physical Security of Plant and Equipment

Included under this subtopic are the physical measures--guards, fences, locks, etc.--which are used to control entrance to the computer facility, and measures taken to protect the computer from damage--fire extinguishers, sprinkler systems, etc.

2. Management Practices

This includes administrative, organizational, and personnel procedures designed to promote security within the activity. Examples are segregation of duties between systems analysts, programmers and computer operators; proper hiring procedures, etc.

3. Systems Security

Hardware, software, communication, and data controls are included in systems security.

4. Contingency Planning

This area is concerned with backup systems which will allow a unit to accomplish its mission even though there is a failure or disruption of the primary system. This is done through the use of alternate facilities and methods which help to minimize the effects of a disruption in the system.

These areas will be more fully discussed in Chapters 5 through 8 of this paper.

The other major topic is office information system (OIS) security. Since OIS security has been included as a requirement in accordance with Reference 4 and has been put under the purview of the ADP Security Officer, it has been included in Section B of this chapter.

B. SECURITY OF OFFICE INFORMATION SYSTEMS

As previously mentioned, Reference 4 directs that security procedures will be implemented for office information systems. To clarify exactly what should be classified as an OIS the following definition is provided.

> Office Information System (OIS). Any electronic system which is designed specifically for the purpose of and is being used primarily for office information applications. Office information applications are those functions normally performed in an office environment dealing with documents--including reports, memoranda, notes, correspondence, letters, messages, files, records, forms, working papers, and other textual information. Office information applications include document preparation (word processing), document storage, document retrieval, document manipulation (sorting, indexing, etc.), and distribution (electronic mail). Office information system equipment (OISE) excludes typewriters, office copy machines, and other devices which have no text editing capability as well as general purpose

> and specially designed ADPE which is designed primarily to be applied through the internal execution of a series of instructions--not limited to specific key-stroke functions, but controlled by a general purpose data processing language--to process a variety of applications such as financial management, logistics, scientific, communications, and the like. (Department of the Navy Definition) [Ref. 4: p. A-13]

Because of the similarities between ADP equipment and OISE, CNO in Chapter 4 of Reference 4 sets out the following policy guidelines for OIS security:

1. OIS will be considered a subset of ADP systems and therefore the ADP Security Officer (ADPSO) will have cognizance over the security of the office information systems;

2. The ADPSO will ensure that an Office Information Security Officer (OISSO) is assigned to each OIS;

3. OIS security violations will be handled in the same manner as for any ADP system with the OISSO reporting violations to the ADPSO;

4. The ADPSO will maintain an inventory of all OIS's which will include, as a minimum, the following information:

   a. Identification of OIS;

   b. Location of OIS;

   c. Name of OISSO;

   d. Data sensitivity level authorized for system (see Chapter II);

   e. System type;

   f. Type of media;

   g. Security mode authorized for operation.

5. The ADPSO will ensure that there is a written security operating procedure for the OIS and that it is available to systems users;

6. Because the Navy Finance Center handles only Level II data (Privacy Act or For Official Use Only data) or Level III data (all other unclassified data), it has the option of either securing its OISs as it does its ADP systems or it can apply the minimum appropriate countermeasures to achieve the security requirements outlined below [Ref. 4: p. 4-2]:

a. Steps will be taken to prevent loss of the OIS from natural hazards, fire, theft, and/or malicious acts;

b. Whenever possible, the manufacturer's specifications for temperature and humidity will be followed;

c. A contingency plan for each OIS will be prepared or, when applicable, a group of OISs can be covered by a single plan;

d. If Level II data is processed in an OIS the following additional requirements must be met:

    1. Countermeasures, including hardware, software, and/or administrative procedures, will be used to prevent unauthorized disclosure, modification or destruction of data;

    2. Audit trails which will include identification of the user, date and time accessed, and file(s) accessed or created will be included;

e. If Level I data is ever entered into an OIS the security requirements referenced in Paragraph 4.3c of Ref. 4 must be implemented.

IV. RISK ASSESSMENT

A. OVERVIEW

ADP risk assessment is a method for quantifying the impact of potential threats on organizations supported by automatic data processing [Ref. 5: p. 5]. Basically, it is a method where risks are identified and quantified as to possible dollar impact over a special period. This allows the activity to determine if it will be cost effective to implement countermeasures to reduce the risk. In this respect, it is much like an auditor dollarizing potential loss areas so that he can focus on the areas that appear to have the greatest amount of possible benefit. Risk assessment is the middle phase in the Risk Management Program consisting of (1) Development of an automatic data processing activity plan, (2) risk assessment, and (3) countermeasure implementation and effectiveness review. The activity ADP security plan was discussed in Chapter II. This chapter will discuss the final two steps of the Risk Management Program. Basically these steps consist of determining what the risks are, the countermeasures available to limit the risks, and the cost effectiveness of implementing these countermeasures.

As is pointed out in this chapter, a number of personnel will be needed on the risk assessment team with the result that the cost of risk assessment may be quite high, and

therefore the activity should budget sufficient dollars for manpower and material for the ADP staff. An additional consideration during risk assessment is that if security measures are too restrictive processing costs may rise and the system may prove cumbersome to the user.

B. BENEFITS

There are three major benefits that an agency receives from performing risk assessment [Ref. 6: p. 9]:

- It provides a basis for deciding whether additional security safeguards are needed;
- It ensures that additional security safeguards will help to counter all the serious security risks;
- It saves money that might have been wasted on safeguards which do not significantly lower the overall risks and exposures.

C. ROLE OF MANAGEMENT

In accordance with Reference 4, a risk analysis must be conducted at each ADP activity. The success of the risk analysis could very well be dependent on top management support. The four following items are needed to ensure the success of the risk analysis [Ref. 5: pp. 5-6]:

- Management support of the project expressed to all levels of the organization;
- Management explanation of the purpose and scope of risk analysis to the team and other applicable members of the organization;
- Management selection of qualified team and formal delegation of authority and responsibility;
- Management review of the team's findings.

As an expression of management interest and to document objectives, responsibilities, and a plan of action and milestones (POAM) for conducting the risk assessment, and to ensure departmental support, Reference 4 recommends that a Risk Assessment Team Charter be issued as an activity notice. A sample Risk Assessment Team Charter is included in Appendix B.

D. COMPOSITION OF TEAM

The third element above, a selection of a qualified team, calls for more elaboration. Just as in an organization where the quality of the people can mean the difference between success or failure of a unit, the same is true of the success or failure of the risk assessment program. The team at a minimum should consist of at least one experienced representative from each of the following functions [Ref. 6: p. 9]:

- The operating unit supported by or having jurisdiction over the data under consideration;
- The programmers responsible for support of the operation or function under consideration;
- The unit responsible for managing ADP operations;
- The system programmers--if the agency has this as a separate function;
- The person assigned the responsibility for overseeing or auditing systems security;
- Those responsible for physical security.

Members do not have to be limited to just these functions. The team may well include participants from the legal and personnel departments or at least consultations with these people about different aspects of security and risk be held.

The team leader should be knowledgeable in security and should understand the relationship of systems in the overall organization. Additionally, he should not be the sole representative from his function. He should not have to fill both the role of team leader and function representative as this may bias him on certain issues and interfere with the objectivity he needs to oversee the complete risk assessment program. FIPS Pub 65 recommends that the team leader be selected from either ADP operations, systems programming (analysis) or internal auditing [Ref. 5: p. 6]. Passages from Sawyer indicate that the internal auditor has to be very careful and can not appear to be "authorizing" a system or dictating controls [Ref. 7: pp. 353-393]. Therefore, it is recommended that the internal auditor not be the team leader, nor a "voting member" of the risk assessment team, as it may well affect his impartiality when it comes time to evaluate the system. However, his insights and expertise are needed in the risk assessment and therefore he should be included for all sessions as a non-voting member. His role should be that of a consultant.

E. DEFINITIONS

In the literature of risk assessment a number of words arise frequently that will be defined here for clarification purposes. These words are threat, vulnerability, and countermeasure.

> Threat. Any circumstance or event with the potential to cause harm to the ADP system or activity in the form of destruction, disclosure, and modification of data, or denial of service. A threat is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of the very existence of the system or activity and not because of any specific weakness. For example, the threat of fire exists at all facilities, regardless of the amount of fire protection available. (DON Definition) [Ref. 4: p. A-17]

> Vulnerability. A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to the ADP system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow the ADP system or activity to be harmed by an attack (DON Definition) [Ref. 4: p. A-17]

> Countermeasure (Also called Safeguard). Any action, device, procedure, technique, or other measure that reduces the vulnerability of an ADP system or activity to the realization of a threat. (DON Definition) [Ref. 4: p. A-6]

Particular note should be taken of the four types of possible harm mentioned under threat--destruction, disclosure, and modification of data, or denial of service. These four types of harm are commonly referred to as impact areas and are a key to the way the Navy performs risk assessment.

F. RISK ASSESSMENT METHODOLOGY

As discussed earlier, risk assessment is a crucial step in the evaluation of an ADP security system. While OPNAVINST 5239.1A lists the three phases of the program as (1) development of an activity ADP security plan, (2) risk assessment, and (3) countermeasure implementation and effectiveness review, it goes on further to list the six actions necessary to satisfy the DON requirements as:

> Step 1. Development of an Activity ADP Security Program (AADPSP) which includes a risk assessment plan of action and milestones (POAM);
>
> Step 2. System User and Software Development Participation. This can be accomplished by proper selection of the risk assessment team.
>
> Step 3. Conducting the Risk Assessment. Selection of the proper risk assessment methodology and implementing it;
>
> Step 4. Countermeasure Selection. Using cost-benefit analysis, select and implement countermeasures until further implementation would produce a negative return. Evaluate the effectiveness of the countermeasures after implementation;
>
> Step 5. Risk Assessment Documentation. Ensure there is complete documentation for the first four steps;
>
> Step 6. Proceed with accreditation process. [Ref. 4: pp. 5-1 - 5-5]

Steps 3 through 5, which occasionally are collectively called risk assessment in some Navy publications, will be discussed in the following sections of this chapter. Steps 1 and 6 have already been discussed in Chapter I. Step 2 was discussed in Section D of this chapter.

G. PRELIMINARY SECURITY EXAMINATION

Before the actual risk assessment methodology is undertaken, a preliminary survey examination should be conducted. The results of this survey will help determine the scope of the risk assessment effort. Using this information, the designated approving authority (DAA) will then determine which of the two basic risk assessment methodologies will be employed [Ref. 4: p. E-1]. Included in Appendix B is a sample format for an ADP security survey.

During the preliminary survey, the following four steps should be taken [Ref. 5: pp. 7-8].

1. Listing of Asset Costs

A determination should be made of the replacement cost of computers, related equipment, buildings, data, etc. In instances where the risk analysis is being done in the systems design phase, both the increased value of data in the complete system and the probable increase in the cost of acquiring it should be considered. Included in Appendix B is a partial list of assets that should be considered under the seven categories that must be considered in ADP security.

2. Listing of Threats

A list should be compiled of threats to the ADP facility and its resources. This list should include any threat that has a realistic probability of occurring. For example, a hurricane would not be a threat to an activity in the midwest because there is almost no chance (nor past

experience) of one coming that far inland. However, a tornado would be a realistic threat in the midwest. If the risk analysis is being done in the system design phase, an effort should be made not only to identify existing threats but also to predict any future ones which might result from the implementation or operation of the system. The following areas should be surveyed for threats [Ref. 5: pp. 7-8]:

- Personnel--hiring and termination procedures, scope and amount of training, quality of supervision at all levels;
- Physical Environment--neighborhood, quality and reliability of utilities, building design, operation and maintenance, physical access controls;
- Hardware/Software Systems--operational availability, change controls, software features, documentation;
- Data Communications--hardware and transmission circuits, procedures to validate and control distribution of messages;
- ADP Applications--technical design, documentation, standards;
- Operations--standards and procedures for source document protection, information dissemination, I/O control, tape library, forms, computer room processing, user interface, housekeeping and maintenance, production control, contingency planning.

3. Listing of Existing Security Measures

A listing of all security measures currently in effect should be made. Next to the security measure should be listed the threat(s) which those security measures help to counteract.

4. Management Review

Upon completion of the above three steps, the results should be immediately presented to management. Using this information, management can install temporary safeguards, if needed, until permanent countermeasures can be effected. Additionally, by using the information in the preliminary security survey, management can direct either of the two methods to be used. Method I is the standard method for use in most Navy ADP environments. Method II is for use in the less complex Navy ADP environments [Ref. 4: p. E-1]

H. METHOD I

1. Overview

This method is more detailed than Method II, provides greater detail, and provides for the interaction of threats and the evaluation of threats by impact areas. The major steps to Method I are:

1. Asset Identification and Valuation,
2. Threat and Vulnerability Evaluation,
3. Computation of the Annual Loss Expectancy (ALE),
4. Evaluation and Selection of Additional Countermeasures, and
5. Continue Accreditation Process [Ref. 4: pp. E-2 and E-3].

2. Detailed Procedures

a. Asset Identification and Valuation

For each asset, fill out a copy of the Asset Valuation Worksheet (Appendix B). When trying to determine

how to differentiate between assets it is helpful to break them down into seven basic categories:

- Software;
- Data;
- Hardware;
- Administrative;
- Physical;
- Personnel;
- Communication.

Guidance concerned with breaking assets down into component parts is given in the following passage. "For each asset defined, all components should be in the same physical area, protected in the same manner and subject to damage by the same threat. If one component of the asset is damaged either all other components should be highly likely to be damaged in a similar manner, or the entire asset should be rendered unusable" [Ref. 4: p. E-4]. The four impacts a threat can have are discussed below.

(1) Modification. This is an unauthorized change. When determining a value for the modification of software or data, the value should be based on the cost to correct the consequences of the modification. Or the value could be based on the cost of locating or recovering from the modification. The value of hardware, administrative, physical or communication assets should be the total cost to detect, locate, and correct the modifications.

(2) Destruction. This involves the loss of the asset. Two costs should be totaled to obtain this value. They are the cost to reconstruct or replace the asset and the costs incurred by the denial of service due to the destruction of the asset. Included in the costs to reconstruct should be appropriate labor charges.

(3) Disclosure. This pertains to the unauthorized release of information to people without the need to know. Classified and Privacy Act data have been assigned a recommended impact value for the effects of disclosure.

TABLE I

GUIDELINES FOR IMPACT OF DISCLOSURE OF SENSITIVE DATA*

FOR OFFICIAL USE ONLY	$1,000
Privacy Act or CONFIDENTIAL	$10,000
SECRET	$100,000
TOP SECRET	$1,000,000

*These values are provided for determining the impact of disclosure of sensitive data. For example, the impact of disclosure of a SECRET data file is assigned a value of $100,000, which corresponds to an impact value rating of 5. These values are only guidelines. The impact of disclosure of classified data, Privacy Act data, and all other data is up to the judgement of the functional user. [Ref. 4: p. E-44]

(4) Denial of Service. This is where users are denied service although there has been no destruction of any assets. An example would be a power outage. In cases of

denial of service, asset impact values should be based on additional costs incurred and penalties assessed due to delays in job completion.

After determining the estimated dollar loss for each of the four impact areas, determine the impact value ratings from the table in section H.2.c of this chapter and enter them in the appropriate boxes at the bottom of the asset valuation worksheet.

b. Threat and Vulnerability Evaluation

In this step the asset valuation worksheets prepared in the previous step are examined and a determination is made as to which threat(s) could cause the impacts indicated. Upon identification of a threat, a threat and vulnerability evaluation worksheet (Appendix B) is completed in the following manner:

- The threat is listed by name;
- The threat is described in general terms;
- Examples of how the threat can exploit current vulnerabilities in the ADP environment are cited. Additionally, existing countermeasures to the threat are listed;
- Using the threats and their impact table from Appendix B as a general guideline, an evaluation is made of which of the four impact areas could be affected by the threat;
- After estimating the frequency of a successful attack for each impact area, use the following figure to determine the ratings to enter in the applicable boxes at the bottom of the threat and vulnerability evaluation worksheet. On the same form, describe the circumstances and vulnerabilities of the ADP activity which permit the threat to exist and document how the frequency of successful attack was estimated.

c. Computation of Annual Loss Expectancy (ALE)

The annual loss expectancy (or exposure) is simply a valuation of the average yearly dollar loss to the activity caused by attacks against its assets. To calculate the ALE, simply take the product of the dollar value loss of a successful attack by a threat and the frequency of occurrence of the threat. The following formula can be used to compute the annual loss expectancy.

$$ALE = \frac{10^{(f+i+3)}}{3}$$

where f = frequency of a successful attack by a threat

i = estimated cost impact of a successful attack [Ref. 5: p. 10]

f and i are determined from the following table.

TABLE II

TABLES FOR SELECTING OF VALUES OF i AND f [Ref. 5: p. 10]

If the estimated cost impact of the event is

$10,	let i = 1
$100,	let i = 2
$1,000,	let i = 3
$10,000,	let i = 4
$100,000,	let i = 5
$1,000,000,	let i = 6
$10,000,000,	let i = 7
$100,000,000,	let i = 8

If the estimated frequency of occurrence is

Once in 300 years,	let f = 1
Once in 30 years,	let f = 2
Once in 3 years,	let f = 3
Once in 100 days,	let f = 4
Once in 10 days,	let f = 5
Once per day,	let f = 6
10 times per day,	let f = 7
100 times per day,	let f = 8

To simplify calculations, these arguments can be used to enter the following matrix and determine the annual loss expectancy.

FIGURE III

COMBINED MATRIX OF i, f AND ALE

i=	f=	Once in 300 years (100,000 days)	Once in 30 years (10,000 days)	Once in 3 years (1,000 days)	Once in 100 days	Once in 10 days	Once per day	10 per day	100 per day
		1	2	3	4	5	6	7	8
$10	1					$300	$3,000		$300k
$100	2				$300	$3,000	$30k	$300k	$3M
$1,000	3			$300	$3,000	$30k	$300k	$3M	$30M
$10,000	4		$300	$3,000	$30k	$300K	$3M	$30M	
$100,000	5	$300	$3,000	$30k	$300k	$3M	$30M	$300M	
$1,000,000	6	$3,000	$30k	$300k	$3M	$30M	$300M		
$10,000,000	7	$30k	$300k	$3M	$30M	$300M			
$100,000,000	8	$300k	$3M	$30M	$300M				

[Ref. 5: p. 11]

As can be seen, calculation of the ALE is relatively simple. Problems arise, however, because one threat may have different impacts on a number of assets. To help simplify the data and arrange it for easier analysis, ALE computation worksheets are used. For each of the four impact areas, a

separate ALE computation worksheet is made out by completing the following steps:

- Identify the impact areas for which the ALE is being computed by marking the appropriate box;
- List the assets and asset impact value ratings (taken from the asset valuation form) across the top of the ALE computation worksheet;
- List threats and successful attack frequency (taken from the threat and vulnerability worksheets) down the left side of the ALE computation worksheet;
- Use the above annual loss expectancy matrix to obtain an ALE for each asset/threat intersection. Enter this ALE;
- Sum the asset columns down and the threat rows across. Ensure total threat and asset values are equal and enter that total in box 8.

Upon completion of the ALE computation worksheet for each of the four impact areas, add their totals to derive the activities' total ALE.

d. Evaluation of Additional Countermeasures

In the evaluation of countermeasures a cost benefit model is used. The cost of installation and implementation of the countermeasures must be less than the decrease in the ALE due to the reduced vulnerabilities. The following steps should be performed to accomplish this evaluation.

Take the completed computation worksheet and locate those threats with the highest values for individual threat ALE--the largest values in the far right column.

Starting with the threats with the highest ALE, identify countermeasures which might be able to substantially

reduce the vulnerabilities which these threats seek to exploit. (Note: Appendix F of OPNAVINST 5239.1A provides a partial list of countermeasures listed by category.)

For each countermeasure offering a substantial reduction in vulnerability, prepare an additional countermeasures evaluation worksheet (Appendix B) by doing the following steps:

1. Enter countermeasure name in section 2 and description of countermeasure in section 3;

2. Estimate the annual cost of implementing the countermeasure. In instances where there is a one-time cost only, divide that cost by the anticipated life (in years) of the countermeasure. Enter in Section 2;

3. Identify the vulnerabilities that the countermeasure would reduce if implemented. Determine which threats would be reduced because of the lower vulnerability. Enter these in column form in section 4;

4. Take the current ALE for each threat off of the ALE computation worksheet and enter in section 5a next to the appropriate threat. This value should be the sum of the ALEs for all four impact areas of the threat being examined;

5. Using new ALE computation worksheets determine and enter new successful attack frequency ratings for the threats for each impact area and calculate new ALEs. Sum these for all four impact areas and enter in section 5b.

6. Subtract the projected ALE from the current ALE and enter in section 6;

7. Sum all of the AOE savings in section 6 and enter the total in section 8;

8. Divide the total in section 8 by the sum of all the figures in section 5b. This is the expected return on investment (ROI) and should be entered in section 7;

9. In section 9 list any proposed countermeasures that may overlap the particular countermeasure under evaluation.

e. Selection of Additional Countermeasures

Now that the additional countermeasures have been evaluated individually, it is necessary to determine what effects the implementation of one countermeasure will have on the effects of the other countermeasures. As a starting point, the countermeasure with the highest ROI is assumed to be implemented and then the effects on the ROIs of the other countermeasures are calculated. To compute these effects, the following steps should be followed.

(1) Sort the additional countermeasure evaluation worksheets, completed in the previous section, by descending order of ROI. List on the additional countermeasure summary listing (Appendix B) the original ROI, annual cost, original ALE savings, and countermeasures in sections 1a, 2, 3a, and 4, respectively. In section 5 make a notation if any of the countermeasures are required by higher authority.

(2) Assume the first countermeasure is in effect and reevaluate the effects of the next countermeasure based on this assumption. Adjust the ALE Savings and ROI as necessary. These figures should be entered in sections 3b and 1b. If the adjusted ROI of the second countermeasure is still greater than the ROI of the third countermeasure, assume that both the first and second countermeasures are in effect and reevaluate the effects and ROI of the third countermeasure. If the adjusted ROI of the second countermeasure is not higher than the ROI of the third countermeasure, evaluate the

effects of the first countermeasure's implementation of the effectiveness and ROI of the third countermeasure. Compare the adjusted ROIs of the second and third countermeasures with the ROI of the fourth countermeasure. Continue in this manner until one adjusted ROI is greater than all of the other adjusted and unadjusted ROIs. Assume this countermeasure is in effect and proceed to reevaluate all other countermeasures based on this assumption. Continue in this manner, always selecting the highest adjusted ROI for implementation, until the ROI or adjusted ROI (whichever is lower) is less than 1 for all remaining countermeasures. At this point a negative return is being obtained for each additional countermeasure. Since the countermeasures are now costing more to install and implement than they are accomplishing in risk reduction, it is not advisable to install any of them. The one exception to this would be those countermeasures that are required by higher authority. All countermeasures that fit into this category should be assigned the highest possible priority regardless of ROI.

(3) A plan of action and milestones for implementing the selected countermeasures should be developed. Using available funds, all countermeasures that have been made mandatory by higher headquarters or that have an adjusted ROI greater than 1 should be implemented. For all unfunded countermeasures with an ROI greater than 1, additional funds should be sought through normal budget channels.

(4) After reviewing the documentation generated during the risk assessment overview, the Designated Approving Authority (DAA) will either grant accreditation, issue an interim authority to operate, or order operations to cease. [Ref. 4: p. 3-1]

I. METHOD II

This method incorporates the same essential steps as Method I, but it does not go into as great a detail nor does it provide for interaction in the impact areas. Therefore, its use is limited to less complex ADP environments. The following procedures should be followed when using Method II.

1. Asset Identification and Valuation

Assets are identified and evaluated in the same manner as in Method I, but the information is entered on a risk assessment matrix (Appendix B) instead of an asset evaluation worksheet.

2. Threat and Vulnerability Evaluation and ALE Computation

To complete this step:

- List the threat by name on the left side of the risk assessment matrix;
- Assign a threat value of low, medium, or high by the guidelines set forth in Table IV. Enter this value in the space marked 'TV';
- To compute the ALE, multiply the asset value by the multiplier corresponding to the threat value (determined in previous step). Enter this value in the risk assessment matrix;
- Sum the rows across and the columns down and record this figure on the form.

TABLE IV

THREAT VALUES

Threat Value	Multiplier
Low (L)	.003
Moderate (M)	.033
High (H)	.33

Definitions:

LOW--The risk of a given threat to a specific asset is assessed as having little or no significant impact on that asset as a result of destruction, modification, or disclosure of data, or denial of service. This assessment is made when the threat is considered to be: (1) very unlikely to occur; (2) not applicable; (3) to have low impact on that asset if it does occur; or (4) the threat is controlled by existing countermeasures.

MODERATE--The risk of a given threat to a specific asset is assessed as having a moderate impact on that asset as a result of destruction, modification, or disclosure of data, or denial of service.

HIGH--The risk of a given threat to a specific asset is assessed as having a very significant impact on that asset as a result of destruction, modification, or disclosure of data, or denial of service. This assessment is made when the threat is considered to have a reasonable likelihood of occurrence and, if it occurs, the impact to that asset would be significant. [Ref. 4: p. E-4]

3. Selection of Additional Countermeasures

Method II also uses a cost benefit model for determining which countermeasures should be installed. The one fallacy of this model is that all vulnerabilities are treated as if they are mutually exclusive. It does not account for the fact that one countermeasure may help to reduce a vulnerability and therefore lower the ROI for another

countermeasure. To determine the countermeasures to employ, complete the following steps.

Identify the threats that have the most potential for damage based upon their ALEs and then determine countermeasures which have the most promise of substantially reducing the vulnerabilities which these threats seek to exploit. Enter these countermeasures in column A of the additional countermeasure selection worksheet in Appendix B.

List the threats acted on by the countermeasure in column B with the original ALE for each threat in column C.

Assign a new threat value with the assumption that the countermeasure has been installed. Use this to compute a new ALE which is then entered in column D.

Subtract the revised ALE from the original ALE and enter in column E. This is the annual savings.

Estimate the annual cost for installing and maintaining the countermeasure. Any one-time cost should be amortized over the useful life of the countermeasure. Enter this cost in column F.

Divide column E by column F to obtain the ROI which is entered in column G.

Assign countermeasure priorities based on mandatory requirements by higher authority and by descending order of ROI.

Implement all countermeasures with an ROI greater than 1 or those made mandatory by higher authority. If

sufficient funds are not available, request more in the budget cycle.

The Designated Approving Authority (DAA), using the documentation generated, will grant accreditation, issue interim authority to operate, or order operations to cease.

J. RISK ASSESSMENT DOCUMENTATION

Copies of the risk assessment documentation will be maintained to support the budget requests, help document the activity ADP security plan, and provide references for future risk assessment documentation. It is important to note that all reports, worksheets, and other documentation pertaining to risk analysis are highly sensitive and should be marked and stored as such. [Ref. 5: p. 15]

Frequency of risk assessment documentation will be kept updated and repeated:

a. At least every five years.

b. When any change is made to the facility, ADP equipment, system software, or application software which affects the overall ADP security posture.

c. When any change is made in operational configuration, data sensitivity, or classification level.

d. When any change is made which appears to invalidate the original conditions of accreditation. [Ref. 4: p. E-17]

K. OTHER CONSIDERATIONS

1. Accuracy of Calculations

Because there are so many variables in determining the frequency and impact of threats, calculations are

usually rounded off to the nearest factor of 10. When trying to dollarize the impact or calculate the frequency of occurrence, it is up to the team to use a combination of historical data, their knowledge of the system and their own expertise and judgment. A lot of time should not be wasted trying to make calculations down to the nearest dollar. As is pointed out in FIPS Pub 65, "There will be no significant difference in the overall exposure whether the damage from a certain event is estimated at $110,000 or $145,000" [Ref. 5: p. 9].

2. Human Frailty

When determining countermeasures, do not count personal integrity as a factor contributing to security. Individuals are under different pressures, both financial and emotional, at different times and therefore their resistance to temptation may be weakened [Ref. 5: p. 14]. Donn B. Parker points out several generalized conclusions about computer crime:

- Employers are more likely to be defrauded by their own employees than by outsiders;
- Generally, employees who defraud their employer do so by using resources to which they have access in their jobs;
- The best way to curtail white collar crime is to remove opportunity and incentives;
- The second best deterrent is the fear of getting caught. [Ref. 8: p. 7]

3. Additional Information

More detailed information concerning risk analysis can be obtained from FIPS Pub 41, which deals with computer security guidelines for implementing the Privacy Act, and from FIPS Pub 65, which is a guideline for ADP risk analysis in the federal government. It should be noted that OPNAVINST 5239.1A is based on the latter reference. Additionally, FIPS Pub 65 contains an example of a risk analysis.

V. PHYSICAL SECURITY

Physical security is an important part of any ADP security plan. Additionally, it has been made a mandatory part of all ADP security plans, as indicated by the following quote: "The ADP activity or network will be externally protected against unauthorized access to entry points, access to data, or damage to the activity" [Ref. 4: p. 1-2]. Physical security is defined as follows:

> Physical Security is the protection of a material entity (property) from disruption of its safe and secure state and is concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft.
>
> a. The use of locks, badges, and similar measures to control access to the central computer facility.
>
> b. The measures required for the protection of the structures housing the central computer facility from damage by accident, fire, environmental hazards, loss of utilities, and unauthorized access. (DON) [Ref. 4: p. A-14]

During the assessment of the need for physical security controls, the risk assessment principles of Chapter IV should be used. When determining whether to implement physical security controls, except those controls required by higher authority, calculations should be performed to determine if the annual cost of the proposed control is less expensive than the reduction in the annual loss expectancy achieved.

There would be no reason to implement a non-mandatory control that cost more than it could save.

A. THREATS AND VULNERABILITIES

As indicated in the preceding definition, physical security measures are installed to lessen the risk of damage from unauthorized access, accidents, fire and environmental hazards, and loss of utilities. Some of the actual physical threats and hazards pertaining to each of these classifications are indicated below.

Deliberate Intrusions

- Theft of physical assets
- Theft of information
- Fraud
- Internal sabotage
- External sabotage
- Riots
- Strikes
- Mischief
- Industrial or governmental espionage

Accidental Losses

- Incompetence
- Curiosity
- Interruptions
- Industrial accident

Natural or Man-made Hazards

- Fire
- Windstorm
- Hurricane
- Tornado
- Lightning
- Earthquake
- Explosion
- Flood
- Water damage
- Snow and ice
- Rain and mud

Utility Outages or Breakdowns

- Power
- Communications
- Air conditioning
- Water
- Steam
- Sewer [Ref. 9: p. 29]

Browne also stated that an agency's susceptibility to physical threats may actually be increased if any of the following conditions are present.

- Intense external competition, with high risk of industrial or national espionage and theft of data.
- Intense internal competition, with resultant high turnover in jobs and even reduction in employment force.
- Low employee morale, with tendency toward disgruntlement.
- Centralization of the DP workload in one data center, with increased exposure to a single disaster.
- Access to the central computer from physically insecure remote locations. In the case of dial-up accessibility, either the capability must be severely restricted by hardware/software controls, or the remote sites must be made physically secure. Direct access by personnel of other departments whose functions involve the use of the computer means that security controls for those departments must be in force.
- Widespread negative visibility of the organization. Certain companies have been targets of antiwar demonstrations or environmentalist protests. Even government

units are susceptible to protests involving privacy, social responsibility, or welfare. Being a sociological phenomenon, this threat is quite variable over time.

- Location of the data processing operation in a high risk enviornment. [Ref. 9: p. 30]

The control measures used to implement physical security can be divided into four major areas. These areas are described in the following four sections by the threats that they attempt to counteract and are access, fire, utilities, and natural disasters.

B. ACCESS CONTROLS

1. Overview

Access controls are defined as "procedures to limit access to sensitive areas" [Ref. 10: p. 83]. When determining which physical access controls to employ, the optimum strategy is to control access at each point from the outer perimeter all the way down to subdividions of the ADP operation. To implement this strategy it is convenient to consider the following four points at which access can be limited [Ref. 9: pp. 30-31].

a. External Perimeter

The first line of defense for a computer facility is usually the fence that separates the ground on which the computer facility is sited from the outside world. In instances where a computer operation shares a building with other activities, a fence at the external perimeter may not be possible nor desirable. The external perimeter helps

deter trespassing and funnels employees, visitors, and the public to selected building entrances [Ref. 10: p. 48].

b. Building Access

The external perimeter funnels all persons to the building entrances, where another screening process should occur. Again, as in the case of the external perimeter, many times when a computer facility is colocated with other activities, screening at this point is limited.

c. Area Access

After an individual is in the building he can still be prevented access to the areas surrounding the data processing function by measures such as badges, locked stairwell doors, elevator restrictions, CCTV, alarmed doors, signs, and guards.

d. Computer Room Access

If an unauthorized individual makes it through the first three barriers, he still has to negotiate access to the computer itself. Devices similar to those used to control area access can be implemented. Additionally, door locks might also be used to limit access. Even within the computer room, access to different functions should be limited--this would especially include access to the tape library. As a minimum, the following areas should be analyzed to determine individuals that should be allowed access.

- Computer room;
- Data storage library;

- Input/output area;
- Data conversion area;
- Programmer areas/file;
- Document library;
- Communications equipment area;
- Computer maintenance room;
- Mechanical equipment room;
- Telephone closet;
- Supplies storage. [Ref. 10: p. 50]

2. Procedures for Determining Necessary Access Controls

When trying to determine which access controls best permit access to the facility by authorized personnel while denying access to others, it is helpful to think about the problem in the following three dimensions:

> People--Specific controls are required for different classes of individuals, such as management personnel, programmers, operators, service engineers, janitors, and others.
>
> Areas--Access points all the way from the outside perimeter of the building into the computer room must be identified and controlled; remote terminal areas also must be controlled.
>
> Time--The above two aspects must be considered in terms of the time of day, e.g., business hour versus non-business hour controls. [Ref. 9: p. 31]

An additional consideration is that the protective measures should be strong enough to achieve stated goals but not so restrictive that they are overly expensive or cumbersome. Any measure so restrictive as to cause a large impediment to work flow may be thwarted by the operating

personnel. For example, a security door which requires complicated opening procedures may soon be left slightly ajar by operating personnel. As previously mentioned, to determine the protection measures needed, the risk assessment methodology outlined in Chapter IV should be employed. The first step in doing this is basically the preliminary security examination. Asset costs should first be listed. Then, all threats that can be lessened by physical access controls should be listed. These threats might include common criminals, political activists, vandals, disgruntled employees, etc. After the threats are listed, all areas within the facility should be defined and tabulated. The tabulation would include a statement of the location, function, access requirements (which people at what times), and criticality (contents or activities which may be targets for wrongdoers) for each area. Upon completion of this step, an assessment of the current security measures should be made by completing the following survey.

Instructions for the Facility Physical Security Survey

A. Obtain a current floor plan which depicts all areas within the facility to include all access points and any adjacent areas belonging to the facility, such as parking lots and storage areas.

B. Begin the survey at the perimeter of the facility and note the following:

    1. Property line to include fencing, if any, and type. Condition, number of openings as to type and use, and how secured. Are there any manned posts at the property line.

2. Outside parking facilities. Is this area enclosed and are there any controls? Is the parking lot controlled by manned posts or are devices used?

3. Perimeter of facility. Note all vehicular and pedestrian entrances and what controls are used, if any. Check all doors--number, how secured, any controls or devices, such as alarms or key card devices. Check for all ground floor or basement windows--how secured; screening, bars, etc., and vulnerability. Check for other entrances such as vents, manholes, etc. Are they secured and how? Check for fire escapes--number and location and accessibility to interior of facility from fire escape (windows, doors, roof). How are accessways secured?

4. Internal security. Begin at the top floor or in the basement. Check for fire alarm systems and devices noting the type, location, and number. Where does the alarm annunciate? Check telephone and electrical closets to see if they are locked. Are mechanical and electrical rooms locked or secured? Note any existing alarms as to type and number. Where do the alarms annunciate? Determine number and location of manned posts, hours, and shifts.

5. Monitoring facility. Location, who monitors, who responds, type, and number of alarms being monitored.

C. The following questions should also be included in a physical security survey:

1. Is the installation/building protected by alarm system(s)?

2. How many zones of protection are within the protected building?

3. Is the alarm system adequate and does it provide the level of protection required?

4. Are there any vulnerable areas, perimeter, or openings not covered by an alarm system?

5. Is there a particular system that has a high nuisance alarm rate?

6. Is the alarm system inspected and tested occasionally to insure operation?

7. Is the system backed up by properly trained, alert protection officers who know what steps to take in case of an alarm?

8. Is the alarm system regularly inspected for physical and mechanical deterioration?

9. Does the system have tamper-proof switches to protect its integrity?

10. Do system(s) have environmental or protective housing or covers?

11. Is there an alternate or separate source of power available for use on the system in the event of external power failure?

12. Where is the annunciating unit located--local, central station, etc.?

13. Who maintains the equipment and how is it maintained (contract, lease equipment, force account personnel)?

14. Is the present equipment outdated?

15. Are records kept of all alarm signals received to include time, date, location, action taken, and cause of alarm?

16. Are alarms generated occasionally to determine the sensitivity and the capabilities of systems? [Ref. 10: pp. 46-47]

After completion of the above steps, risk assessment methodology I should be employed to aid in choosing appropriate countermeasures. The following four subsections contain a discussion of countermeasures currently available for each access point.

3. External Perimeter

There are four main methods for limiting access at the boundary of the ADP site. Each of these has certain

advantages and disadvantages. It may well be that a combination of methods will be needed to provide proper security. [Ref. 10: pp. 47-48]

a. Fences or Other Barriers

These measures will provide crowd control, deter casual trespassers and help in controlling access to entrances. Disadvantages include cost, unsightliness, inability to use in certain areas (such as around the Federal building) and the fact that a determined individual can penetrate it. Additionally, a response force is needed to handle any individuals penetrating the barrier.

b. Intrusion Detectors

Intrusion detectors are usually infrared or microwave beam devices which, when interrupted by an intruder, will result in an alarm sounding. They are cheaper than fences, but are not effective in crowd control, can be circumvented by a determined intruder, and are subject to nuisance alarms caused by unintentional trespassers or false alarms. Additionally, an immediate response force is required upon the sounding of an alarm.

c. Patrol Forces

Patrol forces are most often used when a number of Federal buildings are colocated in the same area but fencing or other barriers are impractical. Patrol forces can provide immediate response, aid in crowd control, and their presence is usually a deterrent to intruders. However,

their cost is prohibitive and intruders can slip in while the force is making its rounds.

d. Closed-Circuit Television System (CCTV)

CCTV allows an individual stationed in a command post to monitor a large area and is usually less expensive than a roving patrol. Additionally, it can aid in crowd control by allowing the individual in the command post to monitor the crowd and send the reaction force to the point needed. Some of its disadvantages are that it is susceptible to electrical failure unless a back-up generator is provided, an inattentive monitor can allow access to go unnoticed, and it requires a response force.

4. Building Access

One of the purposes of the external perimeter is the funneling of persons desiring access to entrance doors where the screening process can occur again. However, an individual desiring unauthorized access is more likely to try an unguarded door, window or other opening instead of going through a door where further screening is required. Therefore, in this section both entrance door controls and perimeter intrusion controls will be discussed.

a. Entrance Door Controls

At an entrance door, personnel can be screened either by a guard or by the possession of a suitable device to unlock the door. The guard, when following strict entrance procedures, constitutes a more effective screening

procedure. A guard does not have to be a uniformed person. It may be a receptionist, clerk, or anyone else who requires an individual to provide identification before permitting entrance. One disadvantage of guards is that often they can be talked into allowing an individual without proper identification entrance if that person can provide a plausible reason. However, guards are especially useful in preventing tailgating. Tailgating occurs when an intruder enters immediately after an authorized entrant. There are three basic methods that can be used for establishing identity for the purpose of admittance [Ref. 11: pp 8=12].

(1) Something Known to an Individual. This refers to a combination that must be entered to obtain access. A disadvantage of this system is that it may be compromised without people being aware of it. There are two types of combination locks currently in use:

Mechanical push button combination locks restrict entrance by allowing access to only those persons who press the correct combination. However, this system does not allow for an audit trail of who entered or the time entered. If there are a number of authorized entry points, either one combination will open every door or individuals may have to memorize a different combination for each door. This reduces the effectiveness of separating ADP functions by different doors and locks. Another disadvantage is that combinations must be changed often and personnel informed of

the new combination. The major advantages to the system are that it is relatively inexpensive and easy to implement.

Electronic combination locks restrict entrance to those persons who key in the correct combination. A number of models with varying capabilities can be obtained. These capabilities range from simple machines that allow access in the same manner as mechanical combination locks to more complicated systems where each individual has his own combination. Through individual combinations the system can lock out specified combinations, limit access to specified times, log all entrances and exits, and control a number of different doors. This overcomes most of the shortcomings of mechanical combination locks but it is much more expensive [Ref. 10: p. 49]

(2) Something Possessed by an Individual. This type of system allows entry to any individual that has a key. The advantage to this system is that only individuals with keys can be admitted. The main disadvantage is that anyone who can obtain a key can enter. There are three basic key and lock systems.

Conventional key and lock sets operate as simply as a regular lock on a door. Advantages are that it is very inexpensive. Disadvantages include the following: locks can be picked; keys can be duplicated; there is no record of who entered or exited; and materials can be taken by anyone possessing a key. [Ref. 10: p. 49]

Pick resistant lock sets have the same advantages and disadvantages as conventional locks except that they are several times more expensive, the keys are harder to duplicate and the locks are harder to pick. [Ref. 10: p. 49]

Electronic key systems consist of encoded cards that actuate electric doors. They can be simple or complex and have many of the same advantages and disadvantages of the electronic combination lock. The various types of electronic key systems are explained in Appendix A to FIPS Pub 83 [Ref. 12]. Pages 13-15 of the same reference detail considerations for badge formatting, preparation, and updating.

(3) Something about an Individual. There are a number of features peculiar to each individual that can be used for identification. Those items currently being used or considered are faces, signatures, fingerprints, hand geometry, voiceprints, ear features, dental characteristics, prints from the bottom of the feet and patterns on the retina of the eye. Of these, only face (appearance), signature, fingerprints, hand geometry and voiceprints are promising as convenient identification techniques at this time [Ref. 11: pp. 10-12]. Appearance would usually be checked by a guard, either in person or through CCTV, who would compare the face of the individual seeking admission to a file picture or identification card. The other devices that use

physiological attributes for identification usually operate in the following manner.

- The individual seeking entrance identifies himself by keying his name or inserting a magnetic card with this information on it.
- The device then pulls from memory a reference profile of the attribute of that individual who is seeking access.
- The measured profile of the applicant is compared to the reference profile and the degree of correlation is obtained.
- The degree of correlation is compared to a preset threshold and a decision to accept (allow entrance) or reject (deny entrance) is made. [Ref. 11: pp. 12-13]

The advantages of this system is that it is flexible enough to allow entrance at selected doors and during certain time intervals, and it is not necessary to remember combinations for doors. Even if a key is stolen and/or duplicated, entrance should be denied. Also a single guard can regulate entry at a number of different entrances by CCTV and remote control. Disadvantages are that it is both expensive and time-consuming. During shift changes delays could be encountered as individuals try to enter the working area [Ref. 10: p. 49]. Another disadvantage is that the accept and reject criteria are complementary. If the accept criteria (degree of correlation) is established at a high enough level to minimize the probability of accepting an imposter (Type II error), the system will reject a high number of authorized individuals (Type I error). However, if the criterion is lowered to reduce the number of

Type I errors, a larger number of unauthorized persons will be allowed access [Ref. 11: p. 13].

An excellent discussion of the evaluation criteria to be considered when selecting a personal identification system is contained in Reference 11.

b. Perimeter Intrusion Controls

All possible entry points of the building--windows, transformer vaults, air conditioning louvres, roof hatches, etc.--should be physically secured or have an intrusion alarm installed. Physical security devices include, but are not limited to, break resistant glass or plastic, metal bars, and screens. In areas where physical security devices are impractical or where an intruder would be able to negate a physical security device unobserved, consideration should be given to installing special intrusion sensors. Examples of common sensors are discussed below [Ref. 10: pp. 49-50].

(1) Window Foil. This is a metallic tape that is attached to glass doors and windows. When the glass is broken, the foil breaks and an alarm sounds. A disadvantage of this method is that a scratch in the foil will also actuate the alarm.

(2) Wire Lacing and Screen. Wire lacing and screen works on the same principle as window foil. Fine wires are laced across door panes, floors, walls and

ceilings. Forced entry through the wire will break a strand and set off an alarm.

(3) Taut Wires. This method is designed to protect internal openings from intruders. A fine strand of wire is strung across internal openings, such as air ducts or utility tunnels, and then tension is applied to the wire. Any change in tension will set off an alarm.

(4) Intrusion Switch. This can be either a magnetic or mechanical device used to protect doors, windows, skylights, and other accessible openings. These devices can be recessed to avoid detection and thus are harder to thwart.

(5) Average Penetration Times. Besides trying to control entrance through already existing openings, consideration should be given to the probability that a determined intruder would be willing to go through a wall. average time needed to go through walls are indicated below:

Wall Construction	Tools Used	Penetration Time
2"x4" studs with 1" siding both sides	Hand brace and electric sabre saw	1.55 minutes
8" cinder block wall	Sledgehammer	1.52 minutes*
8" cinder block wall with brick veneer on one side	Sledgehammer	2.12 minutes*
5½" reinforced concrete	Rotohammer drill and sledgehammer	5.44 minutes*
8" reinforced concrete	Rotohammer drill and sledgehammer	10 minutes approx.*

*Add approximately 1 minute for each reinforcing rod encountered. [Ref. 10: p. 50]

It should be noted that all of these methods are extremely noisy and an attentive security force strategically placed should be able to hear the intruder(s) attempting to gain entry.

5. Area Access

Area access control methods are the same as those measures used to control building access. These methods are designed to control access to the area surrounding the data processing function. [Ref. 9: p. 31]

6. Computer Room Access

Within the computer center, access to a number of areas should be restricted to all personnel except those needing access for the performance of their duties. The areas previously mentioned in Section B.1.d should be analyzed to determine which personnel should be authorized access. Most of the devices and systems discussed in Section B.4 under the topic of "Building Access" can be used to control access to different areas within the computer center. Additionally, a number of detection devices can be used with the computer center to determine access to or occupancy of critical areas during periods when they should be vacant. Two of these items--CCTV and intrusion switches--have already been discussed. Instead of use as a detection device, CCTVs are best used to determine if an intruder is present after an alarm system has registered [Ref. 10: p.

51]. The rest of the detection systems can be divided into the following four classifications.

a. Photometric Systems

These systems detect a change in the level of light in the area which can be caused by an additional lighting source or the absorption of existing light. These systems can only be used in windowless areas or where windows have been covered.

b. Motion Detection Systems

There are three types of these systems, all of which work on the Doppler effect. Waves (sound, ultrasonic or microwave) are emitted and receivers monitor them. When an intruder enters, the frequency changes and sets off an alarm.

(1) Sound. These systems operate in the audible range and at a high decibel which makes it annoying to most humans.

(2) Ultrasonic. These systems operate at a high frequency which is inaudible to most humans, but otherwise is identical to the sound system.

(3) Microwave. This system is similar to the above two systems. The major differences are that microwaves are high frequency radio waves and that by using different antennae, the size of the area to be surveyed can be varied. Also, microwave systems can be used in conjunction with sound or ultrasonic systems.

c. Acoustical-Seismic Systems

(1) Acoustical (Audio). This system uses microphones to listen for intrusion sounds. When an intrusion sound is heard the alarm is set off. Because of its sensitivity to sound it can not be used in buildings which are directly under an airport approach or where new construction is taking place. However, cancellation and discrimination units, which can be added to the system, help reduce nuisance alarms due to airplanes, thunderstorms and other similar noises.

(2) Vibration (Seismic). This system is similar to the acoustical system except microphones are attached to objects such as safes, filing cabinets, windows and walls. Vibration of these objects sets off an alarm. Discrimination equipment can be added to lower the incidence of nuisance alarms.

d. Proximity Systems

This classification includes a number of systems that detect the approach of a person or object. Basically, this is accomplished by the creation of an electric field which, when broken, causes an alarm to be sounded. The proximity system is easily disturbed by mops, pails, or fluctuations in electric current and therefore is subject to numerous nuisance alarms. Because of this, it is usually used in conjunction with other systems instead of as a primary system.

7. Mandatory Access Controls

The following access controls are mandatory in accordance with Reference 4.

a. Level III Data Access Controls

The controls necessary for protection of all Level III data are:

> Physical Protection. Activities will provide physical security for their ADP facilities. The degree of physical security required will vary depending on the physical characteristics of each location, its vulnerability within the ADP environment, and the level of data being processed. A minimum physical security program will address the four basic considerations below. For further guidance and assistance refer to OPNAVINST 5510.45B (NOTAL).
>
> (1) Physical security protection will be provided by implementing a series of physical barriers and procedures, including continual surveillance of the controlled area.
>
> (2) Physical access controls will be implemented to prevent unauthorized entry into the central computer facility and remote terminal areas.
>
> (3) Physical access to data files and media libraries will be restricted to individuals requiring access to perform official duties. [Ref. 4: p. J-3]

b. Level II Data Access Controls

The controls necessary for processing Level II data include those from the preceding paragraph and all of the following:

a. Central Computer Facility

(1) Physical security requirements for the central computer facility area will be commensurate with the highest level and type of data being handled.

(2) If two or more ADP systems are located in the same controlled area, the equipment comprising each system may be located so that direct personnel

access, if appropriate, will be limited to a specific system.

b. Remote Terminal Areas

(1) While the physical and personnel security requirements for the central computer facility area are based upon the overall requirements of the total ADP activity, remote terminal area requirements will be based upon the highest level and type of data which will be accessed through the terminal.

(2) When a peripheral or remote device is to be connected to an ADP system or network processing Level I or II data and is to be operated or used by personnel of an activity that is not responsible for the security of the host ADP system or network, the security measures for the peripheral or remote device and its controlled area will be prescribed by the activity responsible for the security of the host ADP system or network whether or not the peripheral or remote device is approved for handling Level I, II, or III data. Such security measures will be agreed to, formally documented, and implemented before the peripheral or remote device is connected to the ADP system or network.

c. Adjustment of Area Controls

(1) When appropriate, provision will be made to permit adjustment of area controls to the protection required for the level and type of data actually being handled in the ADP system, except that the central computer facility and those components approved for the storage and processing of classified material will not be downgraded below the level required to protect secure communications equipment, to maintain the reliability and security of the ADP system, and to protect essential hardware or software components of the ADP system. [Ref. 4: pp. J-4 - J-5]

C. FIRE CONTROLS

"According to the literature, the biggest threat universally faced by computer facilities is fire. The 1959 Pentagon fire, for example, destroyed $6.7 million worth of

equipment and over 7,000 reels of magnetic tape" [Ref. 9: p. 31]. The threat is twofold to the computer facility, either or both of the computer and building are susceptible to fire. The Design Manual: Fire Protection Engineering (NAVFAC DM-8) prescribes design criteria for fire protection engineering applicable to Naval shore facilities. The Standard Practice for the Fire Protection of Essential Electronic Equipment Operations (RP-1), published by the U.S. Department of Commerce National Fire Prevention and Control Administration, provides guidance to reduce damage caused by fires to computer equipment. This section is based primarily on RP-1, FIPS Pub 31, and those portions of NAVFAC DM-8 that are applicable to electronic equipment and systems. Those portions of the references dealing strictly with the building will not be repeated here.

1. Overview

Fire security is more than just trying to prevent fires from occurring. It includes the measures to detect and extinguish fires before serious damage can occur. When planning fire security the following elements should be included:

- Location, design, construction and maintenance of the ADP facility to minimize the exposure to fire damage.
- Measures to insure prompt detection of and response to a fire emergency.
- Provision of adequate means to extinguish fires and for quick human intervention.

- Provision of adequate means and personnel to limit damage and effect prompt recovery. [Ref. 10: pp. 15-16]

2. Facility Fire Exposure

When determining which fire controls should be installed, it is necessary to know the susceptibility of the facility to fire. This is known as the facility fire exposure and is based on the following five variables. [Ref. 10: pp. 16-17]

a. Occupancy

Occupancy refers to the type of organization in the building. For instance, facilities housing organizations that process textiles, chemicals, or paints are much more susceptible to fires. Therefore, the probability of a fire occurring is usually directly related to the facility occupancy.

b. Fuel Load

Fuel load relates to the probable severity of the fire based on the contents of the building and is a measure of the material burning capability expressed in equivalent units of wood. This is due to the fact that different materials burn for different lengths of time and at different intensities based upon this fuel load. The following table indicates fire severity based upon fuel load.

For typical offices with metal furniture and storage cabinets the fuel load will range from 5 to 15 lbs per square foot. Storage rooms with paper forms and boxed

TABLE V

FIRE SEVERITY BASED UPON FUEL LOAD

[Ref. 10: p. 16]

Fuel Loading (Equivalent pounds of wood per square foot)	Potential Heat Release (Kilo-calories per square centimeter)	Fire Severity (duration in hours)
5	11	0.5
10	22	1
20	48	2
30	65	3
50	110	6
70	152	9

punch cards, or a magnetic tape library will have fuel loads of 50 to 80 lbs per square foot.

c. Construction Type

Construction types affect both the intensity and duration of the fire and relate to the facility's resistance to structural damage. The five basic types of construction are given in order of preferability.

(1) Fire Resistive. In this type of construction the structure of the building is made of noncombustible materials which are further insulated to protect against loss of strength due to a fire.

(2) Heavy Timber. Exterior walls are noncombustible while columns and beams are heavy timber. Since heavy timber burns slowly it is superior in performance to noncombustible.

(3) Noncombustible. The structure is noncombustible but is not protected from the effects of heat. While the building materials will not provide fuel for the fire, the heat from the fire may collapse the structure.

(4) Ordinary Construction. Similar to heavy timber except smaller. The lumber is of smaller proportions and therefore will burn more readily.

(5) Wood Frame. This is normal residential construction using 2" boards for the framework and 1" boards for the sides. This type of facility catches fire readily and is easily destroyed.

d. Construction Details

A number of structural details may be in use in the building which will help retard the spread of a fire.

(1) Fire Walls. These help to divide a structure into separate buildings when calculating fire susceptibility.

(2) Fire Rated Partitions. Fire rated partitions are designed to retard the spread of a fire within a building.

(3) Fire Rated Stairwells, Dampers or Shutters. These items will help to stop fire and smoke from spreading from room to room and floor to floor.

(4) Use of Low Flame Spread Materials. These materials will help keep the fire from spreading rapidly within the facility.

e. Operation of Building

Improper storage of flammable materials and the accumulation of debris, trash or paper allow fire a greater opportunity to occur and spread. Efforts should be made to keep the building well policed.

3. Fire Detection

In spite of all efforts to limit a facility's susceptibility to fire, there is still the possibility of a fire occurring. It is therefore imperative to have a fire detection system that will allow the fire to be controlled before serious damage is done. Most fires go through three stages--ignition (which is often marked by smoldering), the open flame stage, where the fire is spread by direct flame contact only, and finally to the flammable gas stage, which occurs when the air is hot enough to cause adjacent combustible materials to give off flammable gases. The third stage is marked by rapid spreading of the fire and the ignition of nearby materials due to heat radiation. Since it is best to discover and treat the fire before it reaches the third stage, fire detection equipment that works on the principle of raised air temperature is not recommended [Ref. 10: pp. 17-18]. In fact, RP-1 makes automatic smoke detection systems meeting the requirements of NFPA No. 72E, Automatic Fire Detectors, mandatory for equipment, record storage, and raised floor areas [Ref. 13: p. 30]. In order to design an

effective detection system, the following items should be considered [Ref. 10: p. 18]

a. Location and Spacing of Smoke Detectors

As mentioned before, smoke detectors are mandatory in all equipment, record storage and raised floor areas. Consideration should be given to any other potential fire sites including air conditioning ducts and above hung ceilings. When locating smoke detectors, take into consideration the direction and velocity of air flow and the presence of areas with stagnant air.

b. Detection Control Panel

The design of the detection control panel should facilitate the identification of the detector that has sounded. This could be accomplished by a separate light for each area or smoke detector on the control panel. Additional considerations include a secure system that will actuate a trouble alarm if any part of the system fails or in the event of a power outage and prevention of human deactivation of the system. Several fires in computer facilities appear to have been deliberately set and the fire detection system was deactivated prior to the start of the fire [Ref. 10: p. 18].

c. Human Response

Meaningful human response to the alarm is necessary to determine if there is an actual fire, take steps to control/extinguish it, and evacuate the building. Therefore,

there should be provisions for monitoring of the alarm system by someone from the ADP facility or guard force. Additionally, the detector system must be connected to an alarm which will sound locally and also relay the alarm automatically to the local fire department or to an approved central station supervisory service [Ref. 13: p. 25]. Standard Operating Procedures (SOP) should be written which designate functions, and those personnel to perform them, during a fire alarm.

d. Maintenance of System

Smoke detectors are very sensitive and can be activated by dust or other foreign agents. As a result, the sensitivity of the system is often reduced to limit the nuisance alarms. This may result in delayed detection of an actual fire. It is important that smoke detectors be serviced annually by qualified personnel to ensure they are set to the proper sensitivity level and that they are operating satisfactorily. Any system that is not working properly should be corrected immediately.

4. Fire Extinguishment Methods

After the detection of the fire, it is important that it be extinguished quickly to minimize damage. This section contains a discussion of the types of fire-fighting equipment available. There are five basic methods for fire extinguishment available to a computer facility. They are as follows.

a. Portable Extinguishers

Portable or hand extinguishers can be used by agency personnel to control the fire before it gets out of hand. [Ref. 10: p. 18]

b. Automatic Sprinkler Systems

Automatic sprinkler systems can be used to automatically release water from one or more sprinkler heads when the air temperature reaches the design temperature of the head. Heads can be designed to release water anywhere from 135° to 280°F [Ref. 10: p. 19]. Since the sprinkler head works on the principle of heated air, it is mainly a back-up system which is designed to prevent major damage to an ADP installation. Each automatic sprinkler section covering either electronic equipment or record storage areas must include a water flow alarm which will sound locally and shall also sound at the local fire department or at an approved central station supervisory service [Ref. 13: p. 23]. All automatic sprinkler equipment should be installed in accordance with NFPA No. 13, Sprinkler System.

c. Carbon Dioxide Systems

Sufficient carbon dioxide hose reels should be included to reach all ADP equipment. Additionally, all raised floors not exceeding 2,000 cubic feet in capacity should be capable of being flooded with carbon dioxide by these reel hoses. All raised floors exceeding 2,000 cubic feet in capacity should have the capability of being flooded

with carbon dioxide by manually operated fixed pipe systems with underfloor nozzles [Ref. 14: pp. 8-5-13 - 8-5-14].

d. Hose Lines

Hose lines are used by professional fire fighters to attack the fire with water. [Ref. 10: p. 19]

e. HALON 1301

HALON systems will only be used in addition to automatic sprinklers, automatic smoke detection equipment, portable fire extinguishing equipment, and manual response [Ref. 13: p. 26]. A detailed discussion of HALON systems is contained in Paragraph 706 of that reference and Paragraph 2.1.3 of FIPS Pub 31. It should be noted that at the time of this writing NAVFAC had not approved use of the HALON system.

5. Mandatory Requirements

The mandatory requirements for fire prevention, detection, and extinguishment are as quoted below.

> Fire safety. Guidelines concerning fire safety practices are provided by NAVFAC DM-8, Design Manual for Fire Protection Engineering (NOTAL). Employees will receive periodic training regarding emergency actions. Training will include at least power shutdown and startup procedures, use of emergency power, fire detection and alarm systems, use of fire extinguishers, and building evacuation procedures.
>
> (1) Master control switches that shut off all power to the ADP equipment will be installed to override all other electrical controls used during normal operations. Facilities with air-conditioning systems not designed for smoke removal may include their air-conditioning system on the same master control switches. These switches will be located near the main entrance to the ADP equipment area and adequately labeled to prevent accidental shutoff. Master control switches for systems processing

critical applications will be equipped to require a sequential shutdown routine.

(2) Each controlled area will have a sufficient number of portable fire extinguishers. Each extinguisher will be prominently displayed in an unblocked, easily accessible area, no more than 50 feet from ADP equipment. Only carbon dioxide or halon fire extinguishers will be used on electrical fires. All fire extinguishers will be regularly inspected and properly maintained. The number and types of fire extinguishers on hand will be in accordance with local activity fire regulations.

Smoke Detection. Automatic smoke detection capable of early warning will be installed in all areas as required by appropriate instructions.

Cleanliness. Routine cleaning procedures and schedules will be established and adhered to. Personnel assigned to clean around ADP equipment should only be permitted to do so after receiving proper training. An authorized ADP facility representative will be present during the cleaning operation.

(1) Noncombustible wastebaskets with self-closing or tight-fitting covers will be provided in each ADP equipment area. Burn bags required for classified material will be either retained in safes or stored in metal bulk-refuse containers approved by OPNAVINST 5510.1F.

(2) Contributors to dust, lint, and static electricity, such as outer coats, venetian blinds, and throw rugs, will not be permitted in the ADP equipment area.

(3) Air-conditioning filters will be regularly checked, cleaned, and replaced.

(4) Floors will be kept polished, and, if necessary, buffed to a hard finish. Waxes which powder or flake and steel wool buffing pads should not be used. Exercise extreme care when damp-mopping or waxing to avoid seepage of liquids through joints or raised floors.

(5) Carpeted areas will be vacuumed frequently to prevent accumulation of dust. Antistatic carpeting or spray will be used to reduce static electricity. [Ref. 4: pp. J-1 - J-6]

The guidelines from DM-8 that were referred to in OPNAVINST 5239.1A are:

a. Construction. New structures built to house electronic systems should be of fire-resistive or noncombustible construction and cut off from other occupancies by fire-rated walls or partitions. Existing combustible construction should be replaced with noncombustible construction wherever practical and should be cut off from other occupancies by fire-rated walls or partitions. Additional guidance for construction will be found in NFPA 75 Electronic Computer/Data Processing Equipment, NAVFAC DM-23 Communications, Navigational Aids, and Airfield Lighting, and Federal Fire Council Recommended Practices No. 1 Fire Protection for Essential Electronic Equipment.

b. Protection. Electronic systems shall be protected in accordance with NAVMAT INSTRUCTION 11320.8 and the following:

(1) Manually controlled carbon dioxide hose reel systems should be provided in accordance with the requirements of NFPA No. 12, Carbon Dioxide Extinguishing Systems, except as modified herein.

(2) Systems should be two-shot type with minimum of 300 lbs. CO_2 for primary supply and 300 lbs. for reserve. Where the volume of the largest individual cabinet, console, or equipment item requiring protection exceeds 100 cubic feet, additional CO_2 (both primary and reserve) should be provided in accordance with the assumed volume method outlined in NFPA Standard No. 12.

(3) CO_2 hose shall be 3/4 inch and should be limited to 75 feet per reel. Sufficient numbers of hose reels shall be provided to reach all electronic equipment components with one hose giving consideration to equipment layout, aisle arrangements, and other obstructions. Minimum pipe size supplying hose reels should be 3/4 inch. Hose nozzles should be designed for discharge rate of approximately 100 pounds per minute.

(4) Raised floor spaces, not exceeding 2,000 cubic feet in volume, should be protected by total CO_2 flooding utilizing hose reel systems described in the preceding paragraph but with both the primary and reserve supplies of CO_2 increased by not less than 225 pounds each.

(5) Raised floor spaces exceeding 2,000 cubic feet in volume should be protected by two-shot total CO_2 flooding utilizing manually operated fixed pipe systems with underfloor nozzles. CO_2 supply should be independent of the hose reel system with capacity of both primary and reserve supplies.

(6) High pressure 75 lb. cylinders should normally be used to supply hose reel systems and fixed pipe underfloor systems. Beam scale, designed for use with cylinder rack should be provided to permit weighing of cylinders without removal from racks. Where large quantities of CO_2 are required, low pressure storage may be utilized, provided that the installation and maintenance costs are lower and a resupply of low pressure CO_2 is readily available.

(7) Quick-opening valves should be provided in the supply pipes to hose reels and in the supply pipes to underfloor systems. Separate primary and reserve releases should be located adjacent to quick-opening valves. Primary and reserve supplies should not be interconnected, and cascading type activation of cylinders should not be used. Mechanical releases may be cable-type or pressure operated type. Electrical type releases may be used where emergency power is provided.

(8) Operating instructions should be posted at each pair of releases indicating that both the quick-opening valve and a release must be operated in order to deliver CO_2 to hose nozzle or underfloor system. Primary and reserve releases shall be separately labeled. Where underfloor spaces are used as air plenums, instructions should indicate that air supply fans should be shut down prior to the application of CO_2.

(9) Smoke detection systems should be provided in areas where electronic equipment is operated or remains energized without continuous supervision by personnel. Associated underfloor spaces should be similarly protected, except where such spaces are used as air plenums. Detection devices should be of the type which respond to both gaseous products of combustion and smoke and shall be listed by UL, Inc. Alarms should be transmitted to a central location where personnel are in constant attendance.

(10) Provision should be made to transmit alarm signals from all CO_2 and smoke detection systems to the fire department via the station fire alarm system. [Ref. 14: pp. 8-5-10 - 8-5-13]

Figure 1, adapted from RP-1 and referred to in DM-8, is an easy reference for determining fire detection and extinguishment needs. These are recommendations.

D. UTILITIES

The modern conveniences that allow for and help support computer facilities also are potential hazards for these same systems. This section contains a discussion of electric service, heating and air conditioning, communications circuits, and water and sewage. An assessment of the effects of the loss of or the damage to each of these should be made during the risk assessment phase.

1. Electric Service

Electric service can affect ADP operations through quality--the absence of variations from the normal wavelength, or reliability--the number and duration of occasions when the line voltage departs from nominal for periods too long to be considered transient. A variation is considered to be transient when the line voltage is 90% or less of nominal for more than 4 milliseconds or 120% or more of nominal for more than 16 milliseconds. Transients often occur in the morning as energy demands build up. Measurements can be recorded for a period of time to determine the average

AREAS \ PROTECTION SYSTEMS		AUTOMATIC SPRINKLER SYSTEM	AUTOMATIC SMOKE DETECTION SYSTEM	PORTABLE FIRE EXTINGUISHERS AND EQUIPMENT	EMERGENCY CONTROL TEAM	AUTOMATIC HALON 1301 SYSTEM
EQUIPMENT AREAS		R	R	R	R	O
RECORD STORAGE AREAS		R	R	R	R	O
RAISED FLOOR AREAS	UNDER 18" DEPTH	N	R	A*	A	O
	18" - 36" DEPTH	R***	R	A*	A	R***
	OVER 36" DEPTH	R	R	A*	A	O
SPECIAL EQUIPMENT UNITS (ONE OF A KIND ETC.)		**	O**	A	A	O**

KEY

R - REQUIRED
O - OPTIONAL
A - AVAILABLE (IN THE SPACE ABOVE OR NEARBY)
N - NOT REQUIRED

NOTES

* FLOOR LIFTERS REQUIRED

** SPECIAL ENGINEERING REQUIRED

*** EITHER AN AUTOMATIC SPRINKLER OR AUTOMATIC HALON 1301 REQUIRED

Figure 1. Fire Protection Systems for Essential Electronic Systems Quick Reference Chart [Ref. 13: p. 30]

number of transients and outages that occur. This information should be used in the risk assessment.

2. Air Conditioning and Heating

As most ADP people know, computers need to operate in a regulated temperature and environment. Heating and air conditioning can help by accomplishing the following things.

- Maintaining the temperature within fairly close limits. Temperatures above 30° Centigrade can cause permanent damage to hardware.
- Maintaining the proper humidity for ADP operations. Excessive humidity can cause computer cards to swell and feed erratically. Low humidity can affect tape handling, line printers and ADP hardware.
- Maintaining contamination free air. Contamination in the air can cause the heads to crash on a disk drive. [Ref. 10: p. 34]

A complete review of the facility's air conditioning and heating system should be made. Pages 34-39 of FIPS Pub 31 outline procedures for doing this. For those facilities using steam heat, consideration should be given to a system for detecting breaks in a steam pipe as a leak could cause damage by both heat and humidity.

3. Water Supply and Sewage

Water is needed for fire fighting, sanitation and drinking. Considerations should be given to the probability of a broken water pipe that could cause water to get into the computer. Additionally, drains should be equipped with check valves to keep water from backing up out of the sewer system and inundating the computer. [Ref. 10: p. 22]

4. Communications Security

For any system heavily dependent on remote terminals, an analysis should be made of the reliability of the communication system linking the terminals and computer. Specific guidelines are outlined on pages 39-42 of FIPS Pub 31. Communications security also concerns the safe transmission of information so that unauthorized individuals can not obtain access to it. Further discussion of this topic is presented in Chpater VII of this thesis.

5. Mandatory Requirements

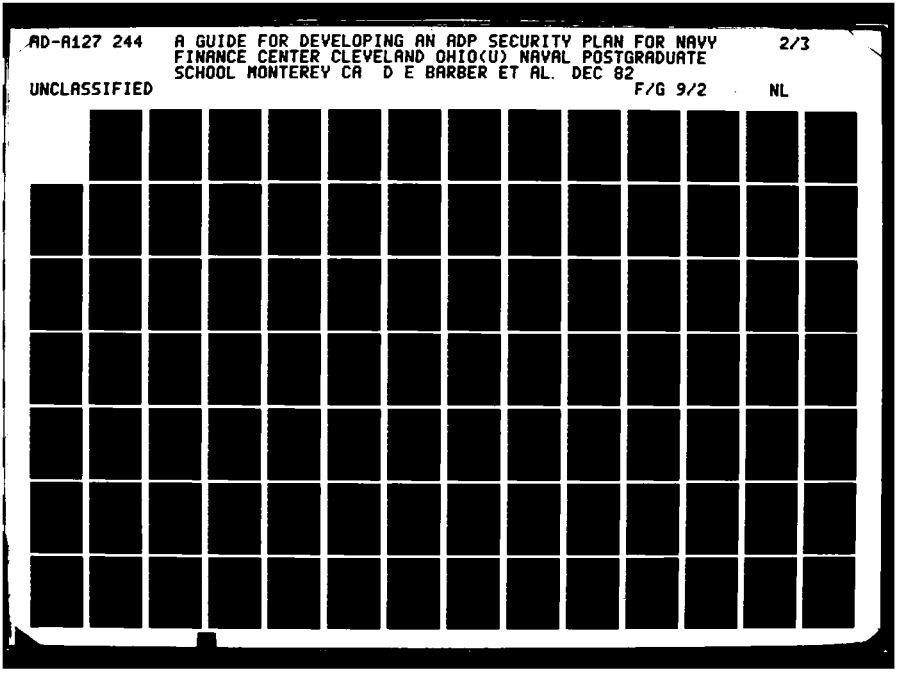
The following requirements are mandatory in accordance with OPNAVINST 5239.1A.

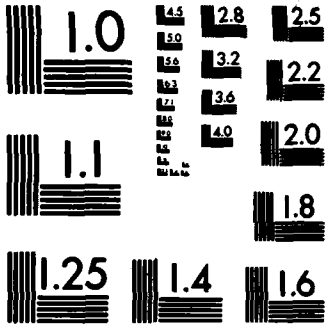
(1) Lighting and Electrical Service. Adequate lighting of the central computer facility and remote terminal areas will be provided and maintained. Emergency lighting will be provided to ensure safe exit in emergencies. Reliable electrical power will be provided. An uninterruptible power source may be required if the facility criticality requires constant ADP support. Voltage regulators or other electronic devices may be necessary to reduce or prevent serious fluctuations in current. Periodic checks will be made of the emergency lighting and the auxiliary power to ensure performance and operability.

(2) Temperature and Humidity. Whenever possible, ADP equipment will be operated within the manufacturers' optimum temperature and humidity range specifications. To prevent excessive temperature and humidity fluctuations, all doors and windows to the central computer facility and remote terminal areas should be kept closed, and only key designated individuals should be permitted to regulate the environmental controls. To maintain a constant record of the temperature and humidity, a recording instrument should be installed and placed where it can monitor the air leaving the ADP equipment area. As a safety feature, an adequate warning system should be installed and maintained

AD-A127 244 A GUIDE FOR DEVELOPING AN ADP SECURITY PLAN FOR NAVY FINANCE CENTER CLEVELAND OHIO(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA D E BARBER ET AL. DEC 82 2/3

UNCLASSIFIED F/G 9/2 NL





warn of near-limit conditions, so that prompt action can be taken to prevent ADP equipment damage.

(3) Precautionary Measures Against Water Damage. False ceilings that conceal steam and water pipes will be checked frequently, and any irregularity will be reported immediately. Work scheduled for the ceiling and raised flooring areas will be coordinated to ensure maximum safety and minimal disruption. Plastic sheets will be readily available to cover the ADP equipment units highly susceptible to water damage. Equipment exposed to water will not be activated until completely dry. [Ref. 4: pp. J-1 - J-2]

E. NATURAL DISASTERS

Natural disasters consist of those elements of nature that may cause damage to an ADP facility. The four that need to be mainly considered are floods, windstorms, thunderstorms, and earthquakes.

1. Floods

The ADP security team should analyze the susceptibility of the facility to flooding. FIPS Pub 31 states that the following areas are most susceptible to floods:

- Riverine flood plains;
- Coastal flood plains;
- Stream areas at the base of a mountain.

If none of the three apply, but the area has a history of flooding, then considerations should still be made to install sump pumps, drains with check valves and other devices designed to minimize flood damage.

2. Windstorms

The two most common windstorms for the United States are hurricanes and tornadoes. While the possibility of a

hurricane doing wind damage to NFC is very remote, the possibility of tornado damage is real. Past experience indicates that several tornadoes are sighted in Ohio each year. The local weather bureau should be contacted to determine the annual probability of a tornado or other high winds in the Cleveland area. This information should be used to determine the annual loss expectancy.

3. Thunderstorms

Thunderstorms often have an effect on the reliability of the electrical service. Calculations should be made of the frequency of thunderstorms and the per cent of times that they rupture electrical service. This information should be included when computing electrical outages. An assessment of the damage to facilities and computer that could be caused by a lightning bolt should also be included.

4. Earthquakes

Earthquakes can cause severe damage to the ADP facility. Figure 3 on page 25 of FIPS Pub 31 indicates that Cleveland is in a zone where only minor damages usually occur. However, it is just a few miles from a zone where major damage is probable. The National Geological Service should be consulted to determine the past occurrence and severity of earthquakes in the Cleveland area.

5. Mandatory Requirements

There are no mandatory requirements concerning natural disasters except for the following:

The effects of natural disasters will be prevented, controlled, and minimized to the extent economically feasible by the use of detection equipment, extinguishing systems, and well conceived and tested contingency plans. [Ref. 4: p. J-3]

VI. MANAGEMENT PRACTICES

There are a number of security measures necessary for an ADP facility that should be performed as part of the management function. These measures can be broadly classified into the categories of personnel and administrative security. These types of measures are not unique to ADP facilities but should be installed for most profit or nonprofit organizations.

A review conducted by Carroll indicates that up until 1977 there have been three distinct phases of criminally motivated computer loss incidents. The first was the assault phase, which mainly involved bombing and arson. Damage resulting from these threats peaked around 1970 and has been declining since that time due to the hardening of computer facilities. The second phase emphasized penetration. This phase consisted of attempts by outsiders to acquire ADP assets by false input documents or falsely obtaining access to time-sharing systems. Losses due to this phase appear to have peaked in the 1972-73 time frame. At the writing of the book (1977) by Carroll the third phase, involving the defection or subversion of employees, was occurring. "These attacks include sabotage as well as theft of every conceivable kind of asset, both by employees and by conspiracies involving employees and outsiders. Embezzlements by insiders

are clearly the leading source of criminal loss today" [Ref. 15: p. 67].

The effective countermeasures to the first phase are primarily the physical security controls discussed in the preceding chapter. The effective countermeasures to the second phase are those physical security measures limiting access to the facility and the systems security measures to be discussed in the following chapter. Damage due to the defection or subversion of employees can be reduced by both physical security measures (limiting movement within the computer facility) and systems security measures. However, management practices consisting of personnel and administrative security are the most effective countermeasures to the defection or subversion of employees.

A. PERSONNEL SECURITY

The importance of personnel controls can not be overemphasized. As one author states:

> All physical, technical, or administrative security measures implemented within a computer system may be rendered ineffective by certain dishonest or careless individuals. It is axiomatic that people represent a company's greatest asset, but from a security point of view they are the biggest liability. The potential threats involving personnel are multifold; they include not only espionage, fraud, embezzlement, and theft, but also inadvertent acts of inexperienced, poorly trained, and careless personnel. [Ref. 9: p. 70]

Personnel security is defined as, "the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is

commensurate with the value of ADP resources which the individual will be able to access" [Ref. 4: p. A-14]. The personnel program of an organization should work to reduce the two vulnerabilities of inconsistent personnel policies resulting in poor employee morale, and a low level of employee training and development [Ref. 9: p. 70].

1. Classification of Personnel Controls

There are three distinct functions that a comprehensive personnel program must address. These functions are personnel selection, personnel training, and supervision of employees [Ref. 10: p. 55]. Each of these functions is critical to a successful program and is the subject of lengthy discourse in the Federal Personnel Manual. Only those parts of the manual pertaining explicitly to ADP functions will be discussed.

2. Personnel Selection

When selecting personnel to fill vacancies, a determination of the candidate's qualifications regarding training, talent and experience to perform the assigned duties should be made. Additionally, when filling sensitive ADP positions, verification of the trustworthiness of the candidate should be made [Ref. 10: p. 55]. The Federal Personnel Manual classifies ADP positions into three categories. Both of the first two categories are considered to be sensitive positions.

(1) Critical-sensitive positions--ADP-I positions. Those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

(2) Noncritical-sensitive positions--ADP-II positions. Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to insure the integrity of the system.

(8) Nonsensitive positions--ADP-III positions. All other positions involved in computer activities. [Ref. 16: p. 732-4.01]

These classifications are elaborated on in subsection 6 of this section. When determining which positions are sensitive, the guidelines from FIPS Pub 31 are useful.

> ...generally these (sensitive positions) will include computer operations, data control, management, auditing and programming (including acceptance testing and maintenance) of critical applications and systems. The risk analysis for fraud will usually identify critical interface points. Wherever a critical interface involves a single individual, the position is probably sensitive. [Ref. 10: p. 55]

3. Personnel Training

> A surprising number of operations problems and security breaches result from promoting an individual into a position beyond his competence. Rather than admit defeat, such people have been known to destroy source documents or falsify reports in an attempt to conceal shortcomings. [Ref. 10: p. 55]

In addition to adequate job training, security training should be continuous. "The purpose of this training is to insure that each individual recognizes his vital role in

installation security and does not--through familiarity--become careless" [Ref. 17: p. 33]. One key to security training is ensuring that personnel are always aware of security considerations. This security consciousness can be transmitted to all personnel by the following devices [Ref. 10: pp. 74-75]:

- Position Descriptions. All ADP position descriptions should contain a detailed list of responsibilities regarding ADP security.
- Employee Orientation. All new employees should receive an ADP security orientation.
- Bulletin Board. A special security bulletin board should be installed on which all new security regulations will be posted. Employees would be expected to initial the regulations after reading.
- Posters. A number of posters concerning ADP security are available. These can be used to serve as a constant reminder.
- News Media. If the organization has a newspaper or circular, articles concerning ADP security should be included.
- How-to-do-it Instructions. Instructions for implementing ADP security plans can be used for training. An example of this might be the written instructions of what each individual is to do in the event of a fire alarm.
- Training. Regular training classes using films, lecturers, seminars, and similar devices should be held to maintain employee awareness of security and to inform them of new threats, vulnerabilities and countermeasures.

As part of the training plan, all employees should be aware that if any of the following conditions occur, it should be reported immediately to the ADP security officer

[Ref. 15: p. 76]. A discussion of ADP security training is presented in Chapter X of this thesis.

4. Supervision

Supervisors can make strong contributions to the security program in the following three ways [Ref. 10: p. 55]:

- He can set the example by complying with security directives and can also ensure his staff complies.
- He can maintain close effective communications with his staff to both identify and reduce the number of disgruntled employees.
- Finally, he can ensure that his subordinates are properly trained and competent.

In addition to the above, there are several other steps that supervisors can take to reduce the opportunity for employee fraud. First of all, supervisors can help control vacations and job rotations. Not only can vacations help reduce errors by maintaining morale and reducing fatigue but they also help deter fraud because the probability of discovery is increased when the perpetrator's job is performed by someone else, even if for only a short period of time. Job rotation reduces risk by improving the level of cross-training. It also helps deter fraud because personnel realize that the next individual who performs that function might discover the fraud. The second step that supervisors can take to reduce employee fraud is to restrict employees from handling their own accounts. When an employee handles his own account he is presented with an unnecessary

temptation. One method of reducing fraud is by removing the opportunity to easily perform a fraudulent act [Ref. 18: pp. 8-9].

5. Termination Procedures

An often overlooked facet of personnel security is the procedures for handling terminated employees. Employees who are terminated, voluntarily or involuntarily, are much more likely to be disgruntled and therefore present a threat to the system. To minimize the vulnerability to the threat, the following steps, if applicable, should be performed.

1. Collect all identification including badges, ID, and business cards (new business cards and ID cards indicating retired status may be considered for retiring employees).

2. Revoke all powers of attorney including bank signature cards. Change or revoke all codes or passwords to which the employee was privy (note that the requirement to be able to do this must be considered when selecting the strategy for assigning passwords).

3. Collect all keys (including magnetic stripe cards), signature plates, and other evidences of authority.

4. Settle all accounts including expense accounts and courtesy accounts.

5. Reconcile accounts of any resource over which the employee had control, such as petty cash, parts inventory, or tape library. Where indicated for the protection of the employee who will assume accountability, an audit should be considered.

6. Reclaim all proprietary information in the custody of the employee.

7. Remind the employee of any ongoing contractual obligations to you, including restrictions on use of data to which the employee has become privy in the course of employment with you. [Ref. 18: p. 9]

6. Mandatory Procedures

The Federal Personnel Manual has issued the following policy for screening Federal personnel associated with the design, operation or maintenance of Federal computer systems and personnel having access to data in these systems. These procedures require that:

(1) In accordance with paragraph 732-1-3 and paragraph 732-A-4 of the Federal Personnel Manual, ADP positions be classified as category I, II, or III;

(2) Personnel be screened in accordance with Chapter 736 of the Federal Personnel Manual and paragraph 16-214 of OPNAVINST 5510.1F, which require that a National Agency Check and Inquiry (NACI) be required for employment in noncritical-sensitive and nonsensitive positions and a pre-appointment full-field investigation be required on applicants for critical-sensitive positions;

(3) That personnel in ADP-I positions be reinvestigated every five years in accordance with paragraph 736-2-6 of the Federal Personnel Manual; and

(4) For all ADP positions a continuing assessment of the trustworthiness and reliability of the incumbents be made by system managers. [Ref. 16: pp. 732-4.01 and 732-A-1 - 732-A-2]

Federal guidelines for designating ADP positions are included in Appendix C.

7. Personnel Audit Checklist

The AFIPS System Review Manual on Security contains an audit checklist on pages 16-24 that can serve as a guide for evaluating the personnel program. It was compiled prior to the publication of the ADP position classification scheme, however, so it does not address those items. [Ref. 19: pp. 16-24]

B. ADMINISTRATIVE SECURITY

> Elaborate security measures designed into the hardware or software of a computer system will not prevent the computer operator from putting two-part paper on a printer and keeping one copy of classified output for himself or herself, nor will they keep an intruder out of the tape library. Basic administrative controls are an integral part of information security in a data processing environment...." [Ref. 20: p. 51]

The preceding quote stresses the need for administrative security controls in an ADP security program. Administrative security is defined as "the management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data. Synonymous with procedural security" [Ref. 21: p. 4]. The proper design and implementation of administrative controls can reduce the following vulnerabilities.

- DP standards are non-existent, or those that exist relate mainly to documentation.
- Security and control standards are poor, unenforced, or do not exist.
- There are no policies, standards, or procedures in relation to protection of privacy in systems which process personal data.
- Controls for data entry and output are not viewed as a challenge by systems people and users. Systems are designed with little consideration of edit checks to prevent data pollution.
- Data entry personnel are not trained or are not evaluated on their ability to catch mistakes and control their own errors.
- There are no controls over the submission, receipt, and output of data in batch processing jobs. [Ref. 9: p. 70]

1. Principles of Security Management

There are three major principles that should be kept in mind during the design of administrative controls. These principles are separation of duties, the never alone principle, and the limited tenure principle [Ref. 15: pp. 46-47].

a. Separation of Duties

The purpose behind the separation of duties principle is best expressed by Enger and Howerton who write, "The responsibilities of users and staff should be divided in such a way that collusion between entirely separate groups--an unlikely circumstance--is necessary in order to compromise the system. Knowledge of the system must be divided and restricted so that few people have enough knowledge to carry out a successful compromise" [Ref. 22: p. 27]. Within this principle there are three subprinciples that should be followed. They are the separation of ADP from the users, the separation of duties within the data processing function, and the maintenance of traditional separations.

(1) Separation of ADP from Users. The data processing function should not be directly responsible to its customer functions but to a common level of management. Additionally, no transactions should originate in the data processing function but should come from the using departments. Finally, the data processing manager should be able to show that all work done by the data processing function and all of

resources consumed by that function were authorized by, and on behalf of, an independent customer [Ref. 18: p. 7].

(2) Separation of Duties Within the Data Processing Function. Within the data processing activity, certain functions should be performed by separate individuals to prevent fraud, or at least to make collusion a necessary condition for the perpetration of fraud. If the organization is large enough, each of the following functions should be performed by a separate person.

- Data entry (e.g., keypunch);
- Operation--job initiation;
- Operation--data input (e.g., tape mounting);
- Operation--data output (e.g., printer operation);
- System programming;
- System library maintenance;
- Application design;
- Application programming;
- Program testing;
- Data definition;
- Library management;
- Scheduling;
- Output distribution;
- Maintenance programming;
- Management [Ref. 18: p. 7].

In the event that the data processing organization is not large enough to warrant different

individuals for each of these above functions and it is necessary to assign several duties to the same individual or group, then no individual or group should be allowed to perform both functions of any of the following pairs.

1. Computer operations and computer programming.
2. Data preparation and data processing.
3. Data processing and EDP quality control.
4. Computer operations and custody of EDP media.
5. Receipt of sensitive or valuable material and transmittal of same.
6. Reproduction, issue, or destruction of sensitive information and the granting of authorization for these acts.
7. Applications programming and systems programming.
8. Applications programming and data-base administration.
9. Design, implementation, and modification of security software and any other function.
10. Control of access credentials and any other function. [Ref. 15: p. 47]

One way to help achieve this separation of duties is by developing an organizational chart reflecting the division of duties and position descriptions that detail what tasks are to be performed by each individual filling a position. Figure 2 is an organization model which demonstrates the principle of separation of duties.

(3) Maintenance of Traditional Separation. Long before the recent emphasis on computer security, auditors had researched and written about the internal controls necessary

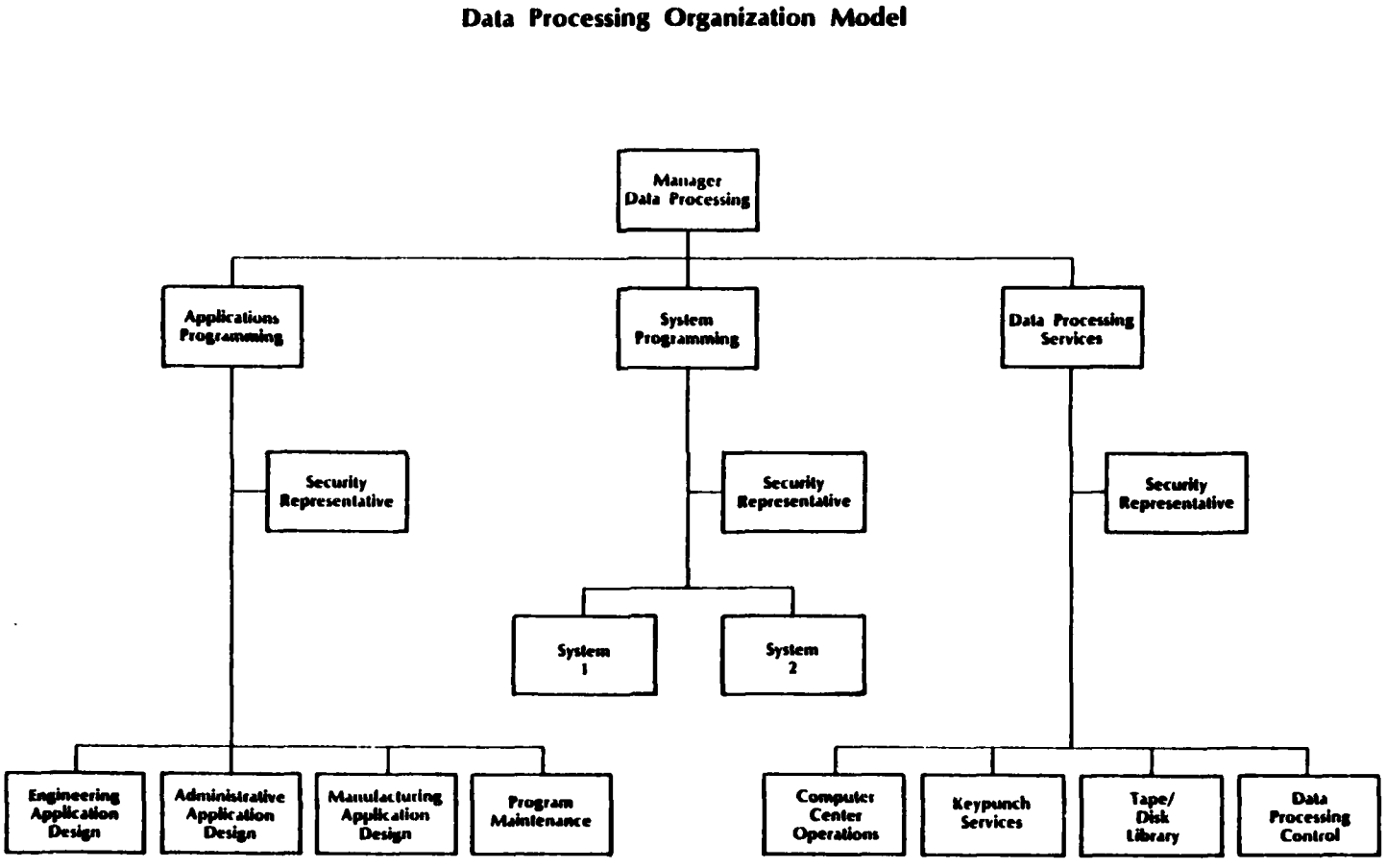


Figure 2. Data Processing Organization Model

in any organization. Arens and Lobbecke list six elements of internal control, the second of which is the adequate segregation of duties. They further break this classification down into the following four categories [Ref. 23: pp. 216-221].

Segregation of the Custody of Assets from Accounting. Any person who has custody of an asset should not also have controls over the records of that asset. Arens and Lobbecke continue:

> In an EDP system, any person with custody of assets should be prevented from performing the programming function, and be denied access to punched cards or other input records. As a general rule it is desirable that any person performing an accounting function, whether it be in an EDP or in a manual system, be denied access to assets that can be converted to personal gain. [Ref. 23: p. 219]

Separation of the Authorizaiton of Transactions from the Custody of Related Accounts. If possible, the person who has control over the assets should not be allowed to authorize transactions concerning the related assets. For example, when preparing a paycheck, the individual who either determines or can change the amount to be paid to an employee should not also be able to sign the check.

Separation of Duties Within the Accounting Function. No individual should be able to enter a new employee's name, check mailing address, pay rate or other vital information without some control for verifying the information being entered. This is for two reasons. First, the control measure will help discover unintentional errors and

secondly, it reduces the chance of an employee entering fraudulent information into the system and collecting the resultant paycheck.

Separation of Operational Responsibility from Record Keeping Responsibility. Record keeping should be performed as a separate function to ensure that departments do not bias the results to show better performance than what was actually attained.

There are two main things that can be done to implement the principle of separation of duties: physical barriers can be erected and rules can be made. The essential physical barriers are:

1. An EDP media ("tape") library must exist in a secure location contiguous to but separate from the computer room.
2. Data preparation (e.g., card punching) must be done in a secure area close to but separate from the computer room.
3. Programmers' offices must be physically separate from the computer.
4. The security office must be a restricted area to all personnel except those directly connected with security.
5. The computer room itself must be a secure area restricted to operators actually on duty or other authorized persons (e.g., maintenance technicians) working under strict supervision.
6. Sensitive waste material awaiting destruction must be stored in a secure area well away from the computer room. [Ref. 15: p. 48]

The methods for making these areas secure have previously been discussed under the topic of access

controls in Chapter V and the section concerning the handling of classified material in Chpater VII. The administrative rules needed to implement separation of duties are:

1. Programmers shall not operate EDP equipment.
2. Operators shall neither write nor submit programs.
3. Implementation and upkeep of security features (that is, modifications to computer operating systems that are intended to enhance EDP security) shall be a separate, distinct duty.
4. Quality control and audit shall exist as functions separate and distinct from EDP production operations. [Ref. 15: p. 49]

b. The Never Alone Principle

This principle helps deter fraud by making it mandatory that two or more individuals attest to or approve certain actions. Based upon the personnel resources of the ADP facility and consistent with the threat evaluation, two or more people should witness certain security-relevant actions. All individuals capable of witnessing the actions should be designated by the Commanding Officer in writing. After witnessing, the individuals should attest to it by signing a memorandum or log. Consideration should be given to applying the Never Alone principle to each of the following actions.

1. Issue and return of access-control items or credentials.
2. Issue and return of EDP media (card decks, tapes, etc.)
3. Systems initialization and shutdown.

4. Processing sensitive information.

5. Hardware and software maintenance.

6. Test and acceptance of hardware.

7. Modification of hardware.

8. Permanent systems reconfiguration.

9. Design and implementation of data bases.

10. Design, implementation, and modification of applications programs.

11. Design, implementation, and modification of operating systems.

12. Design, implementation and modification of security software.

13. Changes to documentation.

14. Changes to emergency or contingency plans.

15. Declaration of a state of emergency.

16. Destruction or erasure of important programs or data.

17. Reproduction of sensitive information.

18. Changes to EDP operating procedures.

19. Receipt, issue, or shipment of valuable material. [Ref. 15: pp. 46-47]

c. Limited-Tenure Principle

This is simply a repeat of the job rotation principle discussed in the personnel section. To reiterate,

> ...crews should be randomly rotated among shifts, individuals should be randomly rotated among crews, mandatory vacation periods should be enforced, and provision should be made for cross-training so that the practice of limited tenure can become a feasible policy. [Ref. 15: p. 47]

2. Security Staff

Figure 2 indicates that each of the three major divisions--applications programming, systems programming, and data processing services--has its own security representative. Although this is preferable, it is not mandatory. OPNAVINST 5239.1A requires only the following four types of security positions on the security staff.

- The ADP Security Officer;
- Network Security officer;
- ADP Systems Security Officer;
- Terminal Area Security Officer.

These positions are the subject of further discussion in both section 2.3 of Reference 4 and Chapter II of this thesis. Therefore, their importance and duties will not be repeated here. It is sufficient to note that they represent administrative controls.

3. Auditing of System

Another form of administrative control is the act of auditing the ADP system. Several auditing establishments are available to perform this function. The first of these is the activity internal review function. By properly conducting internal reviews of ADP functions, internal review officers can spot potential problem areas and allow the Commanding Officer to take appropriate actions to correct the discrepancies. Additionally, if the review is properly documented, Naval Audit Service personnel can use the internal review as

a basis for performing their audit. In accordance with OPNAVINST 5239.1A, internal auditors should place emphasis "on the use of valid audit trails and other management controls in the design and installation of financial and accounting systems. At the local activity level, these functions also include the responsibility to review unique or critical areas related to the safeguarding of resources such as physical security, hardware and software security, and prevention of theft or fraud" [Ref. 4: p. 9-2].

Besides performing audits, the Naval Audit Service is also a valuable source of information on current literature, directives, and events concerning ADP security. Therefore, the ADP security officer should maintain close liaison with the local Naval Audit Service.

4. Administrative Controls

The principle of administrative security has been discussed but specific controls have not been mentioned. This is because they are too numerous to mention. These controls can be generally classified as those that are applied during the various stages of data processing and those that apply to the documentation of systems and programs. The Systems Auditability and Control Study [Ref. 24] and IBM Systems Management: Management Controls for Data Processing [Ref. 25] provide a description of the former controls, and Sawyer provides a listing of documentation requirements for computer programs (Appendix D).

5. Mandatory Requirements

Appendix I to OPNAVINST 5239.1A outlines the security and audit controls applicable to the life cycle of ADP systems. Additional mandatory controls are published in NAVCOMPTINST 7000.36 [Ref. 26].

VII. SYSTEMS SECURITY

The purpose of this chapter will be to discuss systems security development and techniques for hardware, software, data, communications and emanations. Some systems will be combined for ease of discussion in certain areas.

Certain controls cannot be meaningfully discussed or evaluated separately but must be considered as part of an overall system. The hardware, software, data and communications should be considered together when evaluating a security program. For example, hardware and software controls are combined together when processing information to restrict data input and inquiry to authorized individuals. Communications devices, which are used to link hardware components, use software and hardware security controls to provide security. Data is an input to the system, is processed by the hardware using software programs, is transmitted through the communication devices and is an output of the system. Therefore, most hardware, software, communication and security controls should aid in protecting data and thus are also data controls. Although these controls are broken down into different subheadings within this chapter, the reader should be aware that the controls overlap and the implementation of one control may positively or negatively affect the need for a seemingly unrelated control.

A. HARDWARE AND SOFTWARE CONTROLS

Most of the current literature on computer controls discusses hardware and software features together. That procedure will be followed in this section. Hardware security is defined as "computer equipment features or devices used in an ADP system to preclude unauthorized, accidental, or intentional modification, disclosure, or destruction of ADP resources" [Ref. 4: p. A-8]. Software security is the software routines which manage system resources, supervise actions within a system, limit access to files, provide audit trails and achieve other similar security measures [Ref. 9: pp. 92-93].

1. Control Objectives

Mair, Woods, and Davis list four objectives of hardware and software controls. They are as follows:

a. Detection of Errors

Hardware and software controls should be able to detect the following three types of errors:

(1) Errors Generated by the Hardware System. Processing errors can be caused by computer malfunctions, interference, worn out parts, electrical irregularities and other similar incidents.

(2) Errors Within Applications Programs or System Software.

(3) Clerical-Type Errors. These errors are usually made by computer operators or data librarians and involve improper console instructions or the mounting of incorrect files on peripherals.

b. Prevention of Unauthorized Access to and Use of Data and Equipment.

c. Recording of Activities Performed Within the Information Processing Facility.

d. Supporting Effective Utilization of the Computer.

In modern systems, the scheduling and allocation of equipment and jobs is often determined automatically. It is essential that the effectiveness of these hardware and software functions be determined. [Ref. 27: pp. 334-335]

2. Isolation in a Computer System

According to Carroll, the amount of security in an operating system is largely dependent on the isolation of that system. System isolation, in turn, is dependent on the processing mode of that system. The processing mode is dependent on the hardware and software configuration and is determined by the following four attributes.

a. Remote Versus Local

The local processing mode takes place in a secure, controlled access environment for which there is a physically controlled point of access adjacent to the computer. Remote processing consists of all other access environments, including use of remote terminals.

b. Serial Versus Multiprogramming

In serial processing, one job is processed to completion before another job is started. In multiprogramming systems, resources may be shared by two or more jobs simultaneously.

c. Batch Versus On-Line

For batch processing, all data and instructions are submitted to the computer before any job is run. On-line processing allows data and/or instructions to be submitted while the job is running.

d. Programming Versus Nonprogramming

In the programming mode, the user may execute any utility or permanent library program supported by the system. The nonprogramming mode, however, constrains the user to the context of specific programs or pre-established instructions only.

e. Ranking of Processing Modes

Following is a ranking of the processing modes from most secure to least secure:

1. Local, serial, batch, nonprogramming;
2. Local, serial, batch, programming (conventional over-the-counter submission for batch processing);
3. Local, serial, on-line, nonprogramming;
4. Local, serial, on-line, programming;
5. Local, multiprogramming, batch, nonprogramming;
6. Local, multiprogramming, batch, programming;
7. Local, multiprogramming, on-line, nonprogramming;
8. Local, multiprogramming, on-line, programming;
9. Remote, serial, batch, nonprogramming;
10. Remote, serial, batch, programming (an RJE terminal on a serial batch system);
11. Remote, serial, on-line, nonprogramming;

12. Remote, serial, on-line, programming;

13. Remote, multiprogramming, batch, nonprogramming;

14. Remote, multiprogramming, batch, programming (usual RJE mode encountered today);

15. Remote, multiprogramming, on-line, nonprogramming (remote terminal operation as found in NCIC, CPIC, etc.)

16. Remote, multiprogramming, on-line, programming. [Ref. 15: pp. 225-227]

3. Hardware Security Measures

a. Applications

Hardware controls are applied by the equipment manufacturer and therefore vary with the type of equipment and manufacturer. They are designed to ensure that data will be read and recorded accurately by the computer peripherals and that errors will not be caused by flaws in any of the hardware. Mair, Wood, and Davis list the following four ways in which hardware controls can be applied.

(1) In the Design of Equipment Elements. Examples of this type of control would be a write protect ring that protects magnetic tapes from being unintentionally overwritten and circuit breakers that would prevent damage due to power surges.

(2) The Testing of Equipment Configurations Before Use. Manufacturers should ensure compatibility of their equipment with the system being used.

(3) Extensive Preventive Maintenance. Regularly scheduled contractor maintenance can help produce a high level of hardware reliability.

(4) Field Replacement of Parts or Components Which Prove Troublesome. With the advent of miniaturization and microchips, on the spot replacement of component parts has become easier. [Ref. 27: p. 336]

b. Hardware Features that Aid Security

NBS Special Publication 500-33 lists the following hardware features that will help achieve system security.

- Positive, unique device identification--devices attached through the switched telephone network which offer the "hard-wired" self-identification capability or the equivalent. Other devices may be identified through cabling addresses, "station ID" addressing protocols, and so on.
- Devices which offer positive verification of mechanical operations (e.g., seek verification in disk devices).
- A print/display inhibit capability for interactive terminals--automatically controlled by the system.
- Devices to clear the residual contents of buffers, electronic storage areas, and all, or portions, of portable I/O media.
- Processing units which offer read and write protection and two or more privilege states.
- External storage devices designed so that there is no possibility of an "undetected mount" situation.
- External storage devices which offer key-operated locks that prevent unauthorized removal of portable media.
- A line-break sensing capability for all communications equipment. All conditions of potential disconnect/reconnect (such as transient noise or other switched-network disturbances) should be made known to the system so that the system will then be able to invoke device-ID reverification procedures.
- A key-operated power on/off switch for remotely-located devices. Certain devices (particularly intelligent terminals and communicating typewriter devices) may have major functions (such as transmit, receive, typewriter only) controlled independently by key-operated switches or a single key-operated multi-function switch. [Ref. 28: pp. 15-16]

4. Software Security Measures

Software controls can be broken down into two basic classifications--application programs and operating systems. Enger and Howerton also include data base management software in their discussion of software security. That topic will not be discussed in this thesis, however. If the reader is interested in this topic he is referred to Chapter 7 of Reference 22.

a. Application Program Controls

The following exerpt from FIPS Pub 31 provides a thorough discussion of programming controls.

> 6.5. Programming Controls
>
> In line with the recognized objective of generating technically sound programs, the ADP security program should include controls in the areas of program design, acceptance testing and standards. Each of these topics is discussed in the following sections.
>
> 6.5.1. Program Design
>
> There are five major program areas in which design can contribute to security. First is the inclusion of audit trails in the programming process. The basic objective is to make it possible at any point in time to determine the status of a given piece of data. In most cases the systems analysts and system designers will want to involve the auditor in the design phase as he will be able to postulate the optimum placement of audit trails and controls.
>
> The second is the development of a test plan that will consider all possible elements of input, and the interfaces and operational aspects of each new program as part of the program design effort rather than as an afterthought. It is not enough to test a program for ranges of likely input; it should also be tested for improbable, illegal and impossible input. In addition, stand-alone tests usually are not sufficient to establish the adequacy of a given program or module. Not all programs need to meet the

same test criteria; the stringency of the testing should be a function of importance, complexity and sensitivity. Development of written testing guidelines tailored to the needs of the ADP facility is an important step in achieving good control.

The third control area is program change. Programs should be designed to simplify installation of future changes. Every change, even those involving only one statement, should be authorized, approved, and documented with no exceptions. Otherwise, control is lost and the programming process becomes anarchistic. Program library maintenance packages, as mentioned previously, can help in the control and maintenance of program changes. Naming conventions are essential to program change control. The current trend is toward integrated data definitions for all ADP applications, so that every element will be unique.

Controls on the accuracy of data records are the fourth design objective. There are a wide range of possible checks including keypunch verification, computer matching against predetermined legal values for fields, self-checking digits and control fields. Standard design criteria should include the qualitative controls to be included in any new application or any revision of an old application.

Finally, quantitative controls where feasible should also be installed during the design process. These could include control totals, run-to-run counts (hash totals), trailer records, dollar controls, automatic checkpoints/interruption routines, verification of the output and input record counts and the like. Violation of qualitative and quantitative controls should cause error notifications maintained as an error suspense file.

The need for quantitative and qualitative controls should be determined by the risk analysis. If the application is of high value, high risk, or consumes a great deal of ADP resources, these controls should receive more attention than low risk, low visibility applications.

6.5.2. Program Installation

One of the most sensitive points in the programming process is the release of an application to the production system, and its operation against a live data base. Installation of a new program should occur only after thorough program system tests have been completed and approved. The more organizational entities participating in this approval, the better the control. The programmer, a testing or

quality control function, operations, and users should all participate in getting the program from design to final acceptance test and into the live system. However, care should be taken to see that approval does not become a mere ritual. Each program should receive detailed, independent review. Larger ADP facilities may want to consider establishing a separate program test and control group. Smaller ADP facilities would probably be served adequately by defining specific procedures for the installation process to be carried out by an existing group but with as much review and separation of responsibilities as is possible. Again, no program should be accepted without adequate and complete documentation which has been reviewed and approved by an independent body. In case of disaster or non-availability of key programmers, the ADP facility could find itself quite vulnerable to loss if the documentation is inadequate.

6.5.3. Documentation of Controls

The procedural controls over data, operations, system design, programming and acceptance testing already described must themselves be documented if they are to be fully effective. This is often done by preparing documents called procedures manuals, operations and user handbooks, or similar titles. Responsibility for producing the documents may be assigned to a procedures group in a large ADP facility. The small ADP facility may call on individuals to document their particular areas. In either case, the ADP security planner should participate. He should analyze the security objectives of the ADP facility as discussed above to determine the role of the practices or standards in accomplishment of security goals. Based both on these security objectives as well as on ADP management goals, a procedures program should be formulated for the ADP facility. [Ref. 10: pp. 60-62]

b. Operating System Controls

An operating system is defined as:

An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to a user and their programs and play a central role in ensuring the secure operation of a computer system. Operating systems may perform debugging, input-output, accounting, resource allocation, compilation, storage assignment tasks, and other "system" related functions. Synonymous with terms such as "Monitor," Executive," "Control Program," and "Supervisor." [Ref. 4: p. A-13]

Enger and Howerton state that the following security features should be included in an operating system.

- The operating system should maintain an unbroken audit trail. The design should not allow a user to disable audit controls or to access all system information.

- User jobs should not be permitted to read or write outside an assigned storage area, and a user should not be ablt to access the monitor or supervisor mode.

- Maintenance personnel should not be able to bypass security controls while performing maintenance work. At such times the system is vulnerable to errors or intentional acts of the maintenance personnel or anyone else who might also be on the system and discover a vulnerability (for example, microcoded sections of the operating system may be tampered with, or sensitive information from on-line files may be disclosed).

- When restarting after a system crash, the system should verify that all terminal locations which were previously occupied are still occupied by the same individuals. An operating system crash should not expose valuable information such as password lists or authorization tables.

- The operating system should erase all scratch space assigned to a job after the normal or abnormal termination of the job. It should also record that multiple copies of output have been made from spooled storage devices.

- Files should not be read or written without having been opened by a program instruction, and inconsistencies should not be introduced into data because of simultaneous processing of the same file by two jobs.

- The operating system should protect a copy of information as thoroughly as it protects the original.

5. Mandatory Procedures

In accordance with OPNAVINST 5239.1A, the following hardware and software security measures are mandatory.

J.3.4 HARDWARE AND SOFTWARE SECURITY FEATURES. A combination of hardware and software features is essential to provide protection for data stored or processed in a resource-sharing ADP system authorized to process Level I or II data. While all of the following features may not be

available in current hardware or software or a combination thereof, they will be provided at the earliest date that the state of the art permits. The available hardware/ software features outlined below should operate unabridged whenever Level I or II data is contained in the resource-sharing ADP system, and measures will be implemented to provide special controls over the access to or modification of such features. Where possible and practicable, such features should contain two or more independent controls which would have to malfunction simultaneously for a breach of system security to occur.

a. The execution state of a processor should include one or more variables, i.e., "protection state variables," which determine the interpretation of instructions executed by the processor. For example, a processor might have a master mode/user mode protection state variable, in which certain instructions are legal only in master mode. Modification of the protection state variable will be constrained by the operating system and hardware such that a user cannot access information for which the user has no authorization.

b. The ability of a processor to access locations in memory (hereinafter to include primary and auxiliary memory) should be controlled. (For example, in user mode, a memory access control register might allow access only to memory locations allocated to the user by the operating system.)

c. The operation of certain instructions should depend on the protection state of the processor. For example, instructions which perform input or output operations would execute only when in master mode. Any attempt to execute an instruction which is not authorized should result in a hardware interrupt which will permit the operating system to interrupt and/or abort the program containing the illegal instruction.

d. All possible operation codes, with all possible tags or modifiers, whether legal or not, should produce known responses by the computer.

e. All registers should be capable of protecting their contents by error detection or redundancy checks. These include registers which set protection state variables, control input or output operations, execute instructions, or which are otherwise fundamental to the secure operation of the hardware.

f. Any register which can be located by the operating system should also be storable, so as to permit the operating system to check its current contents against its presumed contents. (The term "register" as used in paragraphs e and f refers primarily to index or general purpose registers rather than an isolated address of a single storage location within the computer.)

g. Error detection should be performed on each fetch cycle of an instruction and its operand (e.g., parity check and address bounds check).

h. Error detection (e.g., parity checks) and memory bounds checking should be performed on transfers of data between memory and storage devices or terminals.

i. Automatic programmed interrupt should function to control system and operator malfunctions.

j. The identity of remote terminals for input or output should be a feature of hardware in combination with the operating system.

k. Read, write, and execute access rights of the user should be verified on each fetch cycle of an instruction and its operation.

l. The user should not have access to the operating system. A program operating in a user mode should be prevented from performing system control functions. As much of the operating system as possible should run in the user mode (as opposed to the master mode), and each part of the operating system should have only as much freedom of the computer as it needs to do its job. The operating system will contain controls which provide the user with all data to which the user is authorized access, but no more. If such controls are not feasible, output products will be generated only within the central computer facility under the cognizance of the ADPSSO. As a minimum, the operating system will control:

(1) All transfers of data between memory and on-line storage devices; between the central computer facility equipment and any remote device; or between on-line storage devices

(2) All operations associated with allocating ADP system resources (e.g., memory, peripheral devices, etc.); memory protection; system

interrupt; and shifting between user and master protection modes

(3) Access to programs and utilities authorized to perform the various categories of maintenance (e.g., operations which affect authorized additions, deletions, or changes to data) on the operating system, including any of its elements and files

(4) All other programs (user programs) so that access to data is made via an access control and identification system which associates the user and user terminals in the ADP system with the material being accessed

m. Test and Debugging Programs. For ADP systems authorized to process Level I classified data, user application programs and systems programs which do not violate the security or integrity of the ADP system may be debugged during system operation, provided that such activity is limited to the user mode. All other system software development, experimentation, testing, and debugging will be performed on a system temporarily dedicated for these purposes.

n. Clear System Procedures. Procedures will be available for clearing from the system, or making inaccessible, all Level I classified data during operations without the required protection.

o. Shutdown and Restart. For ADP systems authorized to process Level I classified data, the operating system will provide security safeguards to cover unscheduled system shutdown (aborts) and subsequent restart, as well as for scheduled system shutdown and operational start-up.

p. Other Fundamental Features. The following features of the operating system are also considered fundamental to the secure operation of an ADP system. Unauthorized attempts to change, circumvent, or otherwise violate these features should be detectable and reported within a known time by the operating system, causing an abort or suspension of the responsible user activity. In addition, the incident will be recorded in the audit log, and the ADPSO notified.

(1) Memory/sotrage protection. For ADP systems authorized to process Level I or II data, the

operating system will protect the security of the ADP system by controlling:

(a) Resource allocation (including primary and auxiliary memory)

(b) Memory access outside of assigned areas

(c) The execution of master (supervisory) mode instructions which could adversely affect the security of the operating system.

(2) Memory residue. For ADP systems authorized to process Level I data, the operating system will ensure that Level I data or critical elements of the system do not remain as an accessible residue in memory or on on-line storage devices.

(3) Access controls. For ADP systems authorized to process Level I or II data, access to Level I and Level II data stored within the ADP system will be controlled by the ADPSSO, as required by cognizant authority, or by automatic processes operating under separate and specific controls within the operating system established through hardware, software, and procedural safeguards approved by the ADPSSO.

(4) Labels. For ADP systems authorized to process Level I classified data, all Level I classified data accessible by or within the ADP system will be identified as to its classification and access or dissemination limitations, and all output of the ADP system will be appropriately marked.

(5) Terminal identification. For ADP systems authorized to process Level I data, manual and administrative procedures and/or appropriate hardware/software measures will be established to assure that the terminals from which personnel are attempting to access Level I classified data have been protected and that users are authorized such access. Where a terminal identifier is used, for this purpose, it will be maintained in a protected file.

(6) User identification. Where needed to assure control of access and individual accountability, each user or specific group of users of an ADP system authorized to process Level I or Level II

data will be identified to the ADP system by appropriate administrative or hardware/software measures. Such identification measures will be in sufficient detail to enable the ADP system to provide the user only that data and ADP products which the user is authorized to receive.

q. Application. For ADP systems authorized to process Level I or II data, an audit log or file (manual, automated, or a combination of both) will be maintained as a history of the use of the ADP system to permit a regular security review of system activity. For example, the log should record security related transactions, including each access to a data file and the nature of the access (e.g., log ins, production of accountable outputs, creation of new data files, and all files copied). Each accountable file successfully accessed regardless of the number of individual references during each "job" or "interactive session" should also be recorded in the audit log. Much of the material in this log may also be required to ensure that the system preserves information entrusted to it. [Ref. 4: pp. J-6 - J-10]

B. DATA SECURITY

Data security is defined as "the protection of data from accidental or malicious modification, destruction, or disclosure" [Ref. 21: p. 8].

1. General Principles

FIPS Pub 31 provides the following guidelines on data controls.

Apart from conventional internal controls, the ADP security planner should particularly verify control and protection of data files. Care must be taken to see that information which has been designated as sensitive under Federal regulations is properly safeguarded when it is entered into ADP data files. This may require special handling, segregation or other techniques similar to those used for national security information.

The ADP security planner should also evaluate physical handling of data files at all points. He should examine the flow of data through the ADP facility to identify

points at the input/output interfaces, during handling, and during custodial storage, where controls may be needed to safeguard against possible loss or destruction--and equally important to assure that a loss will be detected. The ADP facility should follow defined procedures in case data is lost. Manual control techniques might include tape/disk movement control forms, inventory logs, authorization for use and special handling for critical items.

The use of a computer system for control of data files deserves special consideration if there are a large number of files. Many vendor supplied tape or disk library management systems provide logging and control of tapes by volume, serial number and name; prevent unauthorized destruction of a data file; and provide automatic backup facilities. Such systems handle both on-line and off-line files.

Similar systems are available to manage a program library. The typical system allows continual modification of a program which is being developed while retaining all previous versions. It protects against unauthorized modification, and helps with the management of program modifications. Such packages, whether purchased or developed in-house can be very useful for management and control of data and program files.

In pre-computer days it was axiomatic to lock up sensitive or important information, ledger books and vital records in a desk drawer, file or safe when not in use. The same principle should also apply to valuable computerized data. The tape library should be locked when unoccupied and unauthorized persons should be excluded. Data safes and vaults, and data control rooms should be protected in accordance with the sensitivity and value of the material (data) stored within. The exposure to magnetic fields should be evaluated realistically and reasonable protective measures taken. Computer printouts should be destroyed in accordance with sound procedures to prevent disclosure. It does little good to develop extensive security controls against theft of data from the computer or programming area and then allow the same information to be available from waste baskets, loading docks or trash heaps. The ADP security planner should be sure that data control requirements are properly reflected in the physical protection program. [Ref. 10: p. 59]

2. Mandatory Procedures for ADP Media Security

ADP media are the various substances, material or devices used to store data or information in an ADP environment

[Ref. 4: p. C-1]. These media include magnetic tapes, disks, diskettes, disk packs, paper tape, punch cards, aperture cards, cathode ray tube (CRT) displays, hard copy output, core storage units, mass memory storage units, printer ribbons, carbon paper, and computer output microfilm/microfiche. The security requirements for ADP media are discussed in Appendix C of Reference 4. The parts applicable to the Navy Finance Center have been extracted and are included below. Additionally, the applicable portions of Enclosure 14 to SECNAVINST 5211.5C [Ref. 29], which states the Department of the Navy guidelines for safeguarding personal information in ADP systems, are included. The Department of the Navy has broken ADP media into two basic categories--each of which has its own applicable security controls.

(1) Working Copy Media--Media that is temporary in nature (retained for 180 days or less) and stays within the confines and control of the activity.

(2) Finished Copy--Media that is permanent in nature and can be released to another activity only if released by other than electrical means.

a. Classification of Media

Currently, the Navy Finance Center has data with two different classification levels--Level II and Level III.

(1) Level II Data. Level II data is unclassified data requiring special protection such as Privacy Act data. Personal information, which falls under the Privacy Act, is defined as:

> ...information identifiable to an individual that is intimate or private, such as information pertaining to an individual's financial, family, social, and recreational affairs, or medical, educational, employment, or criminal history; or information that identifies, describes, or affords a basis for inferring personal characteristics. [Ref. 29: p. 1 of enclosure 14]

The order goes on to state that access to personal information shall be limited to those authorized individuals of DOD agencies that need the information for the performance of official duties.

(2) Level III Data. Level III data is all unclassified data that is not included in Level II data.

Although, technically, Level II data is unclassified, Mr. Duane Fagg, Program Manager of Security, NAVDAC, indicated that many ADP installations within the Department of the Navy treat it as classified data and follow the security procedures for classified data. Therefore, the following guidelines for security controls, security markings, and declassifying and clearing procedures will contain the requirements for both unclassified, Privacy Act, and classified data.

b. Security Controls

These are the minimum essential security controls for ADP media. Additional controls, if needed, can be included.

(1) Unclassified Data. Both working copy and finished media will be controlled by Navy Finance Center SOPs

which will ensure that an "adequate level of protection" is provided.

(2) Privacy Act Data. All intermediate (working copy) and final ADP products shall be controlled. ADP media, both working copy and finished, shall be labeled to warn individuals of the presence of personal information and the need for proper handling. Procedures shall be established for accounting for personal information in a computer facility and for transferring storage media containing personal information. These accounting procedures shall include appropriate inventory control measures which will be documented. For each processing period (shift) a designated person will be responsible for ensuring that the policies for the protection of personal information are enforced. [Ref. 30: p. 6]

(3) Classified Data. Working copy media will be dated when created, marked with the highest classification of any data within, protected and stored in accordance with OPNAVINST 5510.1F and destroyed in accordance with the same reference when no longer useful.

Finished media will be marked in accordance with section 4 of this chapter and controlled and accounted for in accordance with OPNAVINST 5510.1F [Ref. 30].

c. Security Markings

The security marking procedures for unclassified and classified data indicated in Section C.3 of OPNAVINST 5239.1A will be used. Additionally, the below listed security

marking requirements for Privacy Act Data will be followed. [Ref. 4: p. C-3]

Any media that contains personal information subject to the Privacy Act will have the following external warning: "PERSONAL DATA--PRIVACY ACT OF 1974". If the media is classified in addition to containing personal information, a classified label shall be used in lieu of the Privacy Act labeling. Any one or more of the following methods can be used for the warning [Ref. 30: para. II.J]:

- Computer generated page markings that conspicuously identify products as containing personal information.
- Stamps or labels.
- Cover sheets warning that the contents of the product contain information covered by the Privacy Act. These sheets would then be attached to the product. Magnetic storage media would not be subject to this form of marking.

d. Declassifying and Clearing Procedures

Declassifying ADP media is a procedure to erase totally and unequivocally any and all classified information stored on that media. Clearing ADP media is a procedure used to erase classified information but it is not as thorough as declassification procedures. Clearing is done when the media will remain within the facility and is usually done for media which will be reused. Declassification is required for media which is to be released outside the facility [Ref. 4: p. C-5]. Procedures for declassifying and clearing various ADP media are outlined in Sections C.4 and C.5 of OPNAVINST

5239.1A and therefore will not be repeated here. It should be noted that these procedures pertain to classified data and would therefore not pertain to NAVFINCEN unless its Privacy Act data was treated as classified data or it later included classified data in one of its systems. However, SECNAVINST 5211.5C, Section IV, does prescribe the following technical safeguards for Privacy Act data.

(1) The use of encryption devices for the sole purpose of protecting unclassified personal information transmitted over communication circuits or processed on computer systems is discouraged.

(2) When magnetic media is transferred from installations which process personal information, steps must be taken to ensure that personal information is not released as residue on the magnetic media.

(3) One of the following actions should be taken to preclude the unauthorized recovery of temporary personal information on magnetic storage media:

Erasure by degaussing or overwriting;

Use of a dedicated pool of magnetic storage media. [Ref. 29: p. 5 of Enclosure 14]

C. COMMUNICATIONS SECURITY

Communications security is primarily concerned with the attacks upon information in ADP systems where such attacks are not dependent upon gaining access to protected assets. It is defined as:

> ...the protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security,

and physical security of communications security materials and information. [Ref. 4: p. A-5]

Besides preventing unauthorized persons from obtaining information, the system should also be designed to prevent unauthorized individuals from entering false data and to reduce noise that causes errors [Ref. 19: p. 67]. Patrick lists the following general principles that should be followed to help achieve communication security.

General Principle: The physical security of the remote terminal where messages are originated and received is of prime importance. If the terminal and the communications leading to it cannot be secured, use the system only for routine transmission.

General Principle: An unreliable communication system is an unsecure one. The quality and integrity of each link and each terminal must be investigated to ensure low error rates or security cannot result.

General Principle: If intelligent terminals and fully formulated messages are required to live with an unreliable communications system, be sure that the features installed to gain reliability do not also increase the risk of exposure.

General Principle: If store and forward message switching computers are used in your system, audit the design and operation carefully, as these constitute an additional set of exposures.

General Principle: If your transmissions are so precious as to require encryption, engage services of an expert to assist your systems people. It must be assumed that industrial spies are experts in their specialty; you must form a superior team to achieve the protection you seek. [Ref. 19: p. 68]

1. Cryptographic Security

Cryptographic security, which is sometimes referred to as cryptosecurity, is used for classified data control and is concerned with the transformation of the data so as to

make it unintelligible to any unauthorized receiver not having the necessary key to retransform it into intelligible data. This transformation and retransformation of data is usually accomplished by an encryption device. However, the use of encryption devices solely for the purpose of protecting unclassified personal data transmitted over communications circuits is discouraged unless a comprehensive risk analysis indicates that encryption is warranted [Ref. 29: p. 5 of Enclosure 14]. Since it is doubtful that a risk analysis will determine that encryption devices are necessary for NFC Cleveland, they will not be discussed in this thesis. Additionally, data encryption is not 100% secure as it is frequently necessary to deencrypt data when it enters a computer so it can be processed. Thus a security hole is created. If further information is desired, the reader is directed to paragraph 5.5.2 of Reference 6.

2. Emission Security

Emission security, which is also referred to as emanations security, is concerned with preventing undesired signal data emanations from being received and interpreted by unauthorized persons. As with cryptosecurity, emission security is primarily used in conjunction with classified data and therefore will probably not pertain to NFC Cleveland. Additional information on emission security can be found in OPNAVINST C5510.93D.

3. Transmission Security

> ...transmission security is concerned with conducting communication procedures in such a way as to afford minimal advantage to an adversely interested person who is in a position to intercept data communictions." [Ref. 15: p. 139]

Carroll further states that the need for transmission security is especially important when two or more computers and two or more remote terminals are connected to form a network [Ref. 15: p. 153]. A number of subjects are included under the heading of transmission security but two topics are especially stressed. These are the identification of users and locations called from and a determination if the user has the necessary authorization for the information requested or being entered. When designing or reviewing a communications system, hardware and software controls should be considered to perform the following functions:

- Authorize and verify all operator sign-ons.
- Authorize and validate the terminal or node location as well as the device type.
- Use time-of-day authorization codes or other access control checks to authorize access to sensitive system components.
- Test for message sequencing to protect against the "record and replay" threat.
- Provide for message rejection and proper notification if authorization tests are not met.
- Validate routing, addresses, message content, and other format constraints.
- Ensure delivery with positive acknowledgment and feedback.

- Employ checksums and other positive assurances that the message sent was correctly delivered.
- Use time-dependent parameters not included in the plain text message, or relate responses to parameters hidden in a previous request.
- In "query and response" systems, use an element not in the plain text of the query as a factor in the response to validate it. [Ref. 9: pp. 114-115]

4. Physical Security of Communications Materials

Physical security measures have already been discussed in Chapter V. Procedures to control physical access should be applied to the following communication devices:

- Terminals and modems;
- Telephone frame rooms where data are transmitted or received;
- Dedicated communications lines to and from distribution points;
- Communications switching centers;
- Local and remote concentrators;
- All processing nodes in the network. [Ref. 9: p. 114]

5. Other Considerations

Although not listed as a specific part of communications security, as defined by DON, communications integrity should be considered when designing or reviewing a communications system. If the system can not transmit a message accurately and in a reasonable amount of time, it may cause incorrect or untimely data to be processed. The following techniques designed to detect and correct communication line errors should be considered.

- Error detection codes, such as horizontal and vertical parity checks or polynomial check codes.

- Manually-initiated corrective actions, such as direct retransmission, retransmission at slower speeds, or retransmission at a later time.

- Systems-initiated corrective actions, such as automatic retransmission if acknowledgment is negative (NAK).

- Alternative routing schemes, such as those that are a part of most distributed networks.

- Establishment of a technical control center to focus communications system control and maintenance activity. (This approach enhances reliability, centralized performance monitoring, diagnosis, and repair functions. A technical control center is especially valuable in a mixed vendor environment; it helps avoid the usual "finger-pointing." However, due to the highly sensitive nature of such a facility, particular care must be exercised over personnel selection, physical protection, and procedures.)

- Backup and redundancy of essential equipment. The extent and scope depends on the criticality of the communications function and the topology of the network (a distributed network has some inherent backup cabability; a hierarchical network is vulnerable to single-element failures). Ref. 9: p. 114]

6. Mandatory Procedures

OPNAVINST 5239.1A does not list any mandatory procedures for facilities processing Level II data. It does, however, provide a description of a number of available countermeasures in paragraphs F.6 and F.8 [Ref. 4: pp. F-33 - F-43]. Additionally, control measures for message input, transmission, and reception, and accounting are listed in Chapter 7 of Reference 24. As for other control procedures, a risk assessment should be undertaken to determine which controls can be beneficially applied.

VIII. CONTINGENCY PLANNING

The purpose of this chapter is to define an ADP security contingency plan and explain how one is best developed. ADP contingency plan development is discussed in Chapter 7 of OPNAVINST 5239.1A but it shall be amplified upon in this chapter. It should be understood that contingency planning is just a part of the overall ADP security plan.

A. DEFINITION

> Contingency planning is an accepted and recommended management practice which provides for well thought out responses either to preclude or, at least, to mitigate the harmful effects of potential disruptive events. Prior to preparing contingency plans for data processing activities, it is necessary to perform a risk analysis to determine the critical ADP systems and to weigh the threats and vulnerabilities as they relate to the organization. Potential emergency situations can then be anticipated, strategies for coping with them can be developed, and finally, a predetermination of expected responses to each type of emergency can be made. Contingency planning should, of course, include the actions which must be taken in response to major disasters such as floods and hurricanes. However, it is essential to remember that due to their greater frequency of occurrence, minor, more mundane events such as hardware and software failures, and operator errors, cause far greater disruption of service. Contingency planning, if it is to be effective, should include the means to prevent, or to recover from, minor disruptions as well as catastrophic situations. [Ref. 31: p. 3]

B. SUPPORTING REASONS

> The growing dependence during the past two decades of virtually all Federal agencies on ADP resources continues today at an unprecedented rate. This expanding dependence increases the importance of plans to prevent loss of ADP service to vital agency functions and activities.

> Until very recently computers were widely regarded as simply a faster and more cost effective means of performing already established manual procedures. Also, when a computer failure occurred, it was possible to revert to the old manual processes with little more effect on the organization than inconvenience. Today, however, the computer must be considered a means of doing what cannot otherwise be done without it. Further, reverting to manual processes upon loss of the ADP resources, for whatever reason, is usually not practical and often quite impossible. It is critical that management recognize this dependence on the ADP resources in order to fully appreciate its own role in contingency planning. The plans should offer adequate assurance that any reasonably anticipatable interruption of an ADP facility's services will not preclude the continued execution of the agency's mission. [Ref. 31: pp. 3-4]

Besides the logical reasoning in support of ADP contingency planning, there are formal requirements for contingency planning. OPNAVINST 5239.1A requires the preparation, documentation, testing and evaluation of ADP contingency plans, at the least, on an annual basis [Ref. 4: p. 7-1]. Other specific government directives that require contingency plans for ADP activities follow.

- Public Law 93-579 (Privacy Act of 1974), Subsection 3(e)(5) requires that agencies maintaining systems of records subject to the Privacy Act shall: "maintain all records...with such accuracy, relevance, timeliness and completeness as is reasonably necessary...." Further, subsection (3)(e)(1Ø) stipulates that agencies shall: "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity...."

- Federal Property Management Regulations (FPMR). The General Services Administration (GSA) has published comprehensive requirements for ADP contingency planning in 41 CFR, Chapter 1Ø1, subparts 1Ø1-35 and 1Ø1-36, FPMR.

- Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum Number 1, July 27, 1978 contains a wide range of requirements on computer security

including contingency planning. In particular, it requires that each agency must include in its security program policies and responsibilities for assuring that appropriate contingency plans are developed, tested and maintained. [Ref. 31: pp. 5-6]

An ADP contingency plan for any size ADP facility should address, at a minimum, the following three elements:

- Emergency Response--Emergency response procedures to cover the appropriate emergency response to a fire, flood, civil disorder, natural disaster, bomb threat, or any other incident or activity, to protect lives, limit damage, and minimize the impact on data processing operations.

- Backup Operations--Backup operations procedures to ensure that essential data processing operational tasks can be conducted after disruption to the primary data processing facility. (Arrangements should be made for a backup capability, including the needed files, programs, paper stocks and preprinted forms, etc., to operate the essential systems/functions in the event of a total failure.)

- Recovery Actions--Recovery actions procedures to facilitate the rapid restoration of a data processing facility following physical destruction, major damage, or loss of data.

To the extent possible, contingency plan documents should be brief so as to facilitate their usefulness and acceptance by the users. The plan should be tested on a recurring basis and modified as changes in the data processing facility workload dictate. Critical applications should be operated on the backup system regularly to ensure that it can properly process this workload. [Ref. 32: p. 6]

C. CONTINGENCY PLAN DEVELOPMENT

Two things are essential to the development of adequate, cost-effective, and workable contingency plans. First, the mission of the parent organization must be identified. These usually represent a relatively small percentage of the total ADP workload. Second, the resources essential to the accomplishment of these specific functions must also be identified. A formal risk analysis, as described in FIPS PUB 65, Guideline for ADP Risk Analysis, or other similar methodologies, will provide the data

from which identification of both critical functions and critical resources can be derived. Once this is done, preparation of the plan may be begun in a logical, systematic manner. Generally, the plan is developed in three parts--Preliminary Planning, Preparatory Actions, and the Action Plan. [Ref. 31: p. 7]

D. ELEMENTS OF AN ADP CONTINGENCY PLAN

The elements of an ADP contingency plan are as follows:

1. Preliminary Planning (Part One). This part establishes ground rules for the remainder of the plan, i.e., it describes the purpose, scope and assumptions relevant to the plan. It also assigns responsibilities, and describes the organizational strategy for coping with emergencies. The strategies selected will, to a large extent, directly influence the development and amount of detail in the following two parts of the plan.

2. Preparatory Actions (Part Two). This part contains sections which describe how the organization is to respond to an emergency. For example, instructions should be developed which specify how to maintain the contents of off-site storage, how to form backup teams, how to determine applications and system software requirements needed for different situations, and how to establish communications requirements. This part of the plan is prepared in as much detail as possible since it should be read and studied beforehand by those who ultimately must respond to an emergency.

3. Action Plan (Part Three). This part consists of three sections which document what to do when an emergency happens. It is not intended to be a tutorial, but should state concisely the actions necessary to effect the organizational strategies which were selected earlier and documented in part one of the plan. The three sections of this part are:

   a. Emergency Response Actions. This category includes those actions which employees must take immediately upon the occurrence of an emergency to protect lives and other resources. These actions are typically necessary upon the occurrence of major events such as tornadoes, floods, fire and earthquakes, as well as in instances of more common happenings such as power outages, bursting water pipes, etc.

b. Backup Operations Actions. This category includes those actions necessary to effect temporary operations at an alternate location when operations at the home facility are no longer possible for whatever reason. These may entail transportation of files, office supplies, equipment, a variety of other materials, and the employees to the alternate site, and the initiation of ADP operations for an indeterminate period of time.

c. Recovery Actions. This section should describe what must be done to restore permanent operations at the home facility following a disaster or major disruption of service. Included may be plans to rebuild the facility, lease alternate facilities and equipment, etc. [Ref. 31: pp. 8-9]

E. STRATEGIES TO BE USED IN CONTINGENCY PLAN DEVELOPMENT

Strategies that may be used in contingency plan development are as follows:

Strategy 1--No Hardware Backup

Some few organizations need an ADP facility to perform their mission, but will not be seriously harmed if they are completely without it for periods of time possibly as long as two weeks. It is the nature of these operations that they are rarely, if ever, dynamic, transaction-oriented, communications dependent shops. In these few cases in which dependence on ADP is not immediate and critical, it is not unreasonable to assume that the original hardware can be repaired or replaced at the current or another location in time to avoid major loss provided only that other dependencies, such as people, data, and programs, are suitably protected through backup procedures. Believing that backup of hardware facilities is not required is not sufficient justification for ignoring contingency planning. Further, a sound risk analysis must support the conclusion that no backup arrangement is required.

Strategy 2--Mutual Aid Agreements

Mutual aid agreements are at least conceptually possible when one facility can accept, without serious harm to its supported organizations, the critical work of another temporarily inoperative facility. Technically practicable transportability of work between two facilities requires that data and programs from one be acceptable to the other

without other than the most modest change and, preferably, no change at all. Rehearsals are essential, and it should be recognized that they are usually costly, and generate unwelcome disruption to the shop providing backup. The rehearsals must include full operability of the critical systems of the facility which is down. These practice sessions or rehearsals must be thoroughly realistic and not, for example, depend on the use of any resources from the inoperative facility for operation at the backup site. These are very difficult to conduct in a mutual-aid environment. To assure compatibility with the backup system, it is highly recommended that critical applications be run (daily, if necessary) at the backup facility as part of the normal job stream (with test data, files, etc.). Quite often, the site providing the backup support must drop some of its less than critical workload in order to provide the support to another facility. Also, the differences in security requirements between the sites must be considered. For example, clearance requirements at the backup site may preclude the entry of operators from the inoperative facility unless prior clearances have been obtained.

It is difficult at best to make mutual aid arrangements totally reliable. Changes in either system (a highly likely occurrence) may instantly render the arrangement invalid. Further, management shifts may invalidate the arrangements with only short notice leaving a previously supported facility without backup.

While mutual aid agreements are conceptually feasible, they rarely, if ever, prove to be totally reliable. The penalty to the shop needing support of discovering in time of need that backup is not actually available is generally too great to warrant complete confidence in this strategy.

Strategy 3--Contingency Centers

Contingency Centers are facilities established to provide a location into which an ADP organization which has lost its own facility can move temporarily to reestablish its operations, either completely or limited to critical systems only. These centers may be cooperatively owned by several organizations to back up the owners' facilities, or they may be established as profit-making ventures which sell rights to their use through membership fees, dues, and other charges. The evolution of these centers is still quite recent--too recent, in fact, for there to be a large body of experience to support their workability or to provide guidance as to the potential pitfalls to be avoided. Determining the feasibility of using such centers is not complex, does not seem to have hidden pitfalls, and thus

should be relatively easy to do if based upon the results of the risk analysis. There are many situations in which such centers may well be the most cost-effective route to go, while there are others in which they are not an appropriate means of backup. Again, the decision must be made on a facility-by-facility basis.

Strategy 4--One Facility, More Than One Location

This is achieved by having ADP in two geographically separated locations, the smallest of which is large enough to carry the critical workload for the few days needed to reestablish the inoperative facility. This strategy does not imply the installation of excess capacity great enough to carry the critical work--only the physical dispersion of the normal capability into two or more locations. The economic feasibility of this is based on the frequently confirmed assumption that, for the majority of facilities, the critical workload is less than 50% (commonly less than 20%) of the total load so that no increase in total ADP capacity is required. Hardware often does not divide cleanly into two halves, but there is usually no requirement to have precisely 50% at each site. Any split which will suit the need for processing the critical work at either location is adequate, provided, of course, that the backup facility converts its workload to include only its critical functions.

Realization of all of the potential benefits of the two-location option requires that full capability to run critical workload exists at both locations. This generally requires availability of the full range of essential skills to be available at each site. This might, but does not necessarily, mean significant added costs. However, the feasibility of this depends heavily on the size of the operation being considered. [Ref. 32: pp. 14-17]

F. COURSES OF ACTION TO BE USED DURING RECOVERY PHASE

The following courses of action should be considered during the recovery phase of a contingency plan.

1. Repair/Restore Current Facility. ADP Facility Damaged--Backup Facilities Available for Critical Processing.

2. Rebuild Facility at Current Site. ADP Facility Destroyed, No Backup Facility/Hardware Available.

3. Build New Facility at Different Location. ADP Facility Destroyed, Management Not Satisfied with Current Location. [Ref. 32: p. 17]

G. ITEMS TO BE SUPPORTED DURING CONTINGENCY PLAN IMPLEMENTATION

The following items must be supported in case of an emergency and a contingency plan must be put into effect.

1. People;
2. Data;
3. Software;
4. Hardware;
5. Communications;
6. Supplies;
7. Transportation;
8. Space;
9. Power and Environmental Controls;
10. Documentation.

In case of an emergency, each of the above areas should be considered and, hopefully, a plan of action for that area would have been pre-developed.

H. SIZE AND DETAIL OF AN ADP CONTINGENCY PLAN

> The value of a plan is not necessarily proportional to its size. The indiscriminate inclusion of material of doubtful value in the plan will seriously downgrade its usefulness to the organization. While no recommendation is made concerning the length of a contingency plan, most organizations should find that the plan will fit comfortably in a regular loose-leaf notebook. Continuous effort will be required to keep the plan trim and concise, yet sufficiently detailed to communicate the relevant information. [Ref. 31: pp. 9-10]

I. TESTING OF THE ADP CONTINGENCY PLAN

> One of the more important aspects of successful contingency planning is the continual testing and evaluation of the plan itself. Quite simply, a plan which has not been tested cannot be assumed to work. Likewise, a plan documented, tested once and then filed away to await the day of need provides no more than a false sense of security....The test plans should form a formal part of the contingency plan documentation and be as fully subject to the review and approval process as the other sections of the plan. [Ref. 32: pp. 27-28]

A sample outline of a comprehensive contingency plan is included in Appendix C.

From the discussion in this chapter, the reader should understand what an ADP contingency plan is, why it is developed, and the basic ingredients of a sound ADP contingency plan. Training and emergency exercises that are affected by contingency planning are discussed in Chpater X.

IX. COMPLIANCE WITH SECURITY DIRECTIVES

A. COMPLIANCE RESPONSIBILITY

The commanding officer, local front line supervisors, and the ADP security staff are all responsible for ensuring compliance with ADP security directives [Ref. 4: p. 8-1]. It should be noted that, for ADP security, the term "commanding officer" includes contracting officers who are responsible for administering ADP contracts [Ref. 4: p. A-5].

B. SECURITY REVIEW

1. Responsibility

The responsibility to review a command for compliance with security directives is shared by a number of positions and agencies. Commanding officers, including the applicable contracting officers, should review their own agencies at least every three years to ensure compliance with security directives. In addition to the commanding officer's review, auditors, Inspector Generals, personnel from the Naval Investigative Service (NIS) and all other DON agencies and organizations that are involved in investigations, monitoring, review or detection functions at any level include in their programs the evaluation of ADP security programs at DON activities [Ref. 4: p. 8-1].

2. Elements to be Reviewed

The commanding officer's review should be comprehensive and thorough. Emphasis should be placed on the review and testing of contingency plans. The following is a minimum list of items that should be included in the review. Additional items may be included.

1. Risk assessment review;
2. Contingency plans review;
3. Security test and evaluation review;
4. Accrediation documentation review;
5. Fraud, waste, abuse or theft;
6. Accidental or deliberate disclosure of information to unauthorized persons;
7. Risk of financial loss;
8. Infringement on personal privacy or acts contrary to the Privacy Act of 1974;
9. Unauthorized destruction or modification of data;
10. Unauthorized use of DON ADP resources. [Ref. 4: pp. 8-1 - 8-2]

C. SECURITY INCIDENTS

In spite of the best efforts to prevent security incidents--violations of security regulations--they are almost certain to occur. For NFC Cleveland, there are three types of security incidents that are likely to occur. These are disclosures of personal data, major criminal offenses and minor criminal offenses. These latter two types of incidents

are often caused by the violation of the Standards of Conduct, which provides that:

> Naval personnel (military or civilian) shall not directly or indirectly use, take, dispose, or allow the use, taking, or disposing of, Government property or facilities of any kind, including property leased to the Government, for other than officially approved purposes. Government facilities, property, and manpower (such as stationary, stenographic and typing assistance, mimeograph and chauffer services) shall be used only for official Government business. [Ref. 33: p. 7]

The term "Government property" has been interpreted to include computer time.

1. Disclosure of Personal Data

Whenever personal data protected by the Privacy Act of 1974 is improperly disclosed, an incident report will be prepared and submitted in accordance with SECNAVINST 5211.5C [Ref. 4: p. 8-2].

2. Major Criminal Offenses

Major criminal offenses are defined as offenses "punishable under the Uniform Code of Military Justice by confinement for a term of more than one year, or similarly framed by federal statutes, state, local, or foreign laws or regulations" [Ref. 34: p. 1]. All major criminal offenses will be reported to NIS for investigation unless they are susceptible to administrative resolution without the need for professional investigative techniques. Matters that could be administratively resolved by a fact finding body, informal inquiry or administrative audits and are without criminal basis would not be major criminal offenses.

Incidents that could be administratively resolved might have resulted from accident, negligence, incompetency, or some similar non-criminally motivated reason. Included as major criminal offenses is the theft or loss of any serialized government property worth $100.00 or more; or unserialized government property worth $500.00 or more. Value is defined as the greater of current market value or government price list [Ref. 35: p. 1]. It is the commanding officer's responsibility to immediately report all major criminal offences to the nearest Naval Investigative Service field component [Ref. 34: p. 1].

3. Minor Criminal Offenses

Minor criminal offenses are defined as offenses "punishable under the Uniform Code of Military Justice by confinement of 1 year or less, or carrying similar punishment by federal, state, local, or foreign statute or regulation..." [Ref. 34: p. 2]. When minor criminal offenses occur the investigation capabilities of the command should be used. Examples of these organic investigations are military police, provost marshals, and security or guard forces. Off base investigation activities, other than the normal liaison with local law enforcement agencies, shall be held to a minimum and should pertain only to the immediate area surrounding the installation [Ref. 34: p. 2].

D. PROBLEM REPORTING

Any unusual or difficult security problems that occur during the administration of the security program should be reported to the Naval Data Automation Command (NAVDAC). Although it is not mandatory that these reports be signed, a signature would aid NAVDAC in determining if the problem was widespread or restricted to a specific system or command. Reports should be in sufficient detail to concisely describe the problem and offer any recommended solution. These reports should be sent to the address listed in paragraph 11.3 of Reference 4.

X. ADP SECURITY TRAINING PLAN

A good ADP security plan is only as effective as the training plan that supports it. Chapter 10 and Appendix D of OPNAVINST 5239.1A are excellent guides to ADP security training. In this chapter, an attempt will be made to illuminate the high points of OPNAVINST 5239.1A with respect to security training while integrating security test and evaluation procedures into the plan.

A. RESPONSIBILITIES

> Commanding officers are responsible for taking appropriate action to provide their ADP security staff with the training and experience required. The depth of knowledge and degree of experience required in the ADP security staff are dependent on the size and complexity of the ADP environment and the level of data being processed.
>
> Each member of the ADP security staff (after being properly trained) is charged with ensuring that activity personnel are adequately trained in ADP security. [Ref. 4: p. 10-1]

B. FORMAL ADP SECURITY TRAINING

> Two 40-hour ADP security courses will be offered in support of the Department of the Navy security program. The first 40-hour course will be a basic course covering ADP security policy, risk assessment, accreditation, and requirements/plans for contingency planning. The second 40-hour course will be more advanced for GS 334 11/13's and includes audit/inspection techniques and procedures and case studies on performing an internal audit, IG inspection, and ST&E. It is planned to conduct courses on-site at the Navy Regional Data Automation Centers. Course information may be obtained from the nearest NARDAC. [Ref. 4: p. D-1]

The first action that should be taken after security staff members are identified should be to send as many of these personnel as possible to these formal training courses. The greater the depth of knowledge and the more widespread it is, the stronger the ADP security program at an individual activity will be.

C. TARGET TRAINING AUDIENCE

The following personnel are included in the target training audience for ADP security:

1. Customers/users;
2. Top management;
3. Security staff:
   (a) ADPSO;
   (b) ADPSSO;
   (c) TASO;
   (d) NSO;
4. Audit staff;
5. IG staff;
6. Procurement staff. [Ref. 4: p. D-2]

Basically, anyone that uses or benefits from the facility should be aware of ADP security. This is why it is important for the Commanding Officer to actively show his support in the development of a sound ADP security program.

D. TOPIC AREAS TO BE COVERED

Suggested topic areas are as follows:

1. General security awareness;
2. User security;
3. Security administration;
4. Change control and computer abuse;
5. Software security;
6. Telecommunication security;
7. Terminal/device security;
8. Systems design security;
9. Hardware security;
10. Physical security;
11. Personnel security;
12. Audit;
13. Data security;
14. Risk assessment;
15. Contingency/back-up planning;
16. Disaster recovery;
17. Security accreditation;
18. Security Test and Evaluation (ST&E);
19. ADP security and Navy interface. [Ref. 4]

These ADP security training areas are more fully developed in Appendix D of Reference 4. Methods of training and persons responsible for conducting the training are further delineated in Figure 10-1 of Reference 4.

E. NFC ADP SECURITY ENVIRONMENT

What is the environment at the NFC, Cleveland? Like many other Department of Defense (DOD) activities, security awareness is only beginning to spread. There is only a small nucleus of personnel with any professional training in ADP security. This is why ADP security training with emphasis on security awareness must be the initial step toward a realistic ADP security plan at the NFC.

The small nucleus of personnel with some computer security expertise must be expanded to include a sufficient number of people to form the first formal ADP security staff at the NFC. This group must be the experts in ADP security for the NFC. In order for this group to become experts, they must first be afforded the opportunity of formal ADP security training. It is recommended that as many members as possible of the ADP security staff should attend the aforementioned 40-hour courses on ADP security that are offered by the DON. Security staff development should not hinge upon the availability of billets for projected staff members to attend the formal courses offered by the DON. Other DOD and DON activities listed in Chapter 10 of Reference 4 will provide ADP security training assistance upon request.

F. SUGGESTED ADDITIONAL TRAINING MATERIALS

Training provided by external command sources should be prefaced by some selected readings on the subject of ADP

security. Establishing a library of readings on ADP security would be a good goal for the first group of potential ADP security staff members. In addition to Reference 4 and its bibliography as potential sources of information, the following readings and their bibliographies are suggested for review:

1. A thesis prepared by Philip A. Myers that is titled Subversion: The Neglected Aspect of Computer Security. [Ref. 36]

2. The Marine Corps Automatic Data Processing (ADP) Security Manual (Marine Corps Order P5510.14) that is dated 2 January 1981. [Ref. 37]

After the initial ADP security staff has achieved sufficient training to give them creditability, it will be their task to coordinate an active ADP security training plan for the remainder of the command.

G. ADP SECURITY TRAINING PLAN DEVELOPMENT

There are six basic requirements that should be considered in the development of an ADP security training plan. Besides overall ADP security awareness, it has been suggested that there are five basic requirements that should be considered for ADP systems that handle or process classified information. It may be debated that, since the NFC processes only Privacy Act data which does not qualify as classified, it is felt that these five requirements may apply to the NFC ADP facility. The five requirements are as follows:

Requirement 1--Marking

An ADP system which is used to process or handle classified or other definitely categorized sensitive information shall clearly store and maintain the integrity of classification or other sensitivity marking labels for all information. The system shall assure that the classified or other sensitive information is accurately marked when included in output from the ADP system. [Ref. 38: p. 8]

Requirement 2--Mandatory Security

The computer system must be able [to] enforce the formal system of information control reflected in the security classification designation and special handling restriction set associated with the sensitive information handled or processed by the ADP system together with the clearance set associated with the individuals who may request access to the information. [Ref. 38: p. 9]

Requirement 3--Discretionary Security

The computer system must be able to enforce access limitations placed on classified or other sensitive information based on identified individuals or groups of individuals who have been determined to have a Need-to-Know for the information. [Ref. 38: p. 10]

Requirement 4--Accountability

An ADP system which is used to process or handle classified information shall make provision for individual accountability whenever classified information is generated or accessed. [Ref. 38: p. 11]

Requirement 5--Continuous Protection

The security relevant portions of a trusted computer system must be maintained under continuous control to assure that unauthorized changes have not been made which could possibly subvert the system's ability to control classified information. [Ref. 38: p. 12]

It is suggested that these five requirements serve as areas to be considered in the development of the NFC ADP security training plan. Although the five requirements are discussed with equal importance, the requirement of

accountability must be understood by all persons, clearly established, and appropriate action should be taken when accountability responsibilities are not maintained.

How does Security Test and Evaluation (ST&E) interface with the establishment of an ADP security training plan? Before answering this question, we should more clearly establish the purpose of ST&E.

> Security Test and Evaluation (ST&E) is a part of the Accreditation process. The primary purpose for conducting an ST&E is to obtain technical information to support the DAA's decision to accredit an ADP activity or network. [Ref. 4: p. 6-1]

With purpose established, the first step of ST&E requires individuals with knowledge of the following:

1. ADP security;
2. System software/hardware;
3. Application software;
4. Telecommunications;
5. Emanation security;
6. Physical security;
7. Personnel, procedural and administrative security;
8. User/customer functions. [Ref. 4: pp. 6-1 - 6-2]

H. TRAINING INTERFACE WITH SECURITY TEST AND EVALUATION (ST&E)

The list of knowledge required of individuals to perform a ST&E overlaps with the subjects in a well-developed ADP security training plan. With the goal of ST&E being ADP facility accreditation, the importance of a good ADP security

training plan is more clearly established. With the requirement for ADP facility accreditation to be re-established at a minimum of once every five years [Ref. 4], the importance of a continually updated active ADP security training plan is emphasized. An active ADP security training program should ensure that any ADP facility be able to pass ST&E requirements and maintain facility accreditation.

The purpose of this chapter has been to identify subject areas that should be included in an ADP security training plan, show the relationship between ST&E and ADP security training and provide some suggested sources of ADP security.

XI. AUDITING

A. PURPOSE

The purpose of this chapter is to establish the need for an effective internal audit program to monitor ADP security. Internal audit program development and implementation will be discussed. Further discussion will be provided on procedures that can be used in preparation for an audit conducted by external auditors.

There are two types of auditors that will be discussed. They are external and internal auditors. The external auditor is anyone that is not from the immediate organization, the NFC, Cleveland, Ohio. External auditors with which NFC Cleveland, Ohio would be primarily concerned are General Accounting Office (GAO) and Naval Audit Service (NAVAUDSVC) representatives. "Internal audit within the DON is the responsibility of the Naval Audit Service (NAVAUDSVC)" [Ref. 4: p. 9-1], but for the purposes of this paper the NAVAUDSVC will be considered external to the NFC.

OPNAVINST 5239.1A establishes the relationship between NAVAUDSVC and GAO where their two primary standards for audit of ADP systems are the same [Ref. 4: p. 9-2]. This seems like a logical situation and the establishment of an

internal ADP audit organization at the NFC with the same standards would be a natural progression of events.

B. INTERNAL AUDIT

1. Supporting Reasons

OPNAVINST 5239.1A clearly states that "external audit and audit assistance are not intended as substitutes for continuing review of ADP security" [Ref. 4: p. 9-3]. It goes on to establish five basic objectives for the internal auditor. Objective 5 should be of particular interest to NFC personnel in support of the establishment of an activity ADP internal audit program. Objective 5 is as follows:

> Objective 5. To provide assurance that ADP systems/applications conform with applicable legal requirements. Early and continuing auditor review in the design and development process should confirm compliance with legal requirements through adoption of countermeasures, controlled responses to information requests, and conformance with adopted standards. Examples include State and Federal statutes, Freedom of Information Act, DOD and DON directives, and Federal Information Processing Standards (FIPS). [Ref. 4: p. 9-4]

The following quote from a GAO report further establishes why we need a strong internal audit program.

> Federal agencies are placing heavier and heavier reliance on computers, with a proportionate increase in vulnerabilities. The consensus of Government and industry computer security experts is that computer security audit, as a function of agency internal audit, should be recognized as a key element in a system of management control. Agencies fall short of making this important provision for management control. [Ref. 39: p. 48]

In further amplification of the objectives or purpose of the internal audit function, the following is applicable.

Internal audit organizations should become involved in the design, development, and test phases of a new computer system as a normal part of the audit function to help ensure that adequate security is built in before a new system goes into operation. Since technical controls usually are an integral part of the whole system, and can not easily be retrofitted at a later date, these early phases in the system's life-cycle are the optimum time for control safeguards to be incorporated. Independent internal audit involvement is highly desirable to ensure that factors to enhance auditability, audit trails for security, and quality output are designed and developed into new systems. Emphasis during these stages may otherwise be on operational priorities and implementation time goals at the expense of the above goals. [Ref. 39: p. 49]

2. Problems in Establishment of Internal Audit Function

With the objectives or purpose clearly established, why should there be a problem with the establishment of a viable ADP internal audit organization?

A primary reason for lack of significant internal audit involvement in computer security was that most agencies' audit organizations do not have adequate personnel with ADP expertise. Officials of seven agencies informed us that their ADP capabilities ranged from no qualifications to perform indepth security type reviews to limited abilities.

We found little evidence of use of outside contracted resources to increase internal audit capability. In one instance, we were told the reason was that the audit group did not even have the expertise to specify tasks and parameters within which consultants could operate.

Our September 1977 report on the low incidence of computer audit conducted in executive agencies cited auditors' lack of technical ADP knowledge as a barrier to performing effective ADP audit by the organizations whose involvement was found to be inadequate. We recommended to heads of agencies that they develop adequate expertise in their internal audit organizations. We found that previously cited deficiencies are still prevalent. This is of increasing concern since agencies' operations are becoming heavily committed to computers, and computer technology is in a dynamic state needing constant monitoring and review. [Ref. 39: p. 50]

With the mandate to establish an ADP internal audit program and the problems of establishing a program very clear, what course of action must be taken by NFC Cleveland, Ohio to solve its problems and establish a viable internal audit function? The assumption has been made that the problems at the NFC are similar to those at other government agencies.

3. Internal Audit Plan Development

The first step that must be taken is to identify the potential members of an internal ADP audit staff. Once identified, the professional qualifications of each potential member must be carefully reviewed and deficiencies in professional expertise should be identified. It is anticipated that obtaining additional professional training for members of this group will become a high priority item. It is recommended that the internal ADP audit staff remain autonomous from the command ADP security staff. While good communication links should be established between the ADP security and audit staffs, it is felt that the two staffs must remain visibly separate in order for the audit staff to maintain an image of credibility and continue to perform its function objectively. It is recommended that as soon as possible, even before all members of the audit staff are identified, that additional outside professional training be arranged for staff members. It should be emphasized to audit staff members that additional professional training will be

an ongoing endeavor in the rapidly changing environment of ADP. Governmental agencies lack personnel with ADP security expertise and will continue to lack personnel with expertise if an ongoing educational program is not established at each individual command. Who can the NFC obtain assistance from in the area of audit program development? The NFC may request assistance from the NAVAUDSVC headquarters or one of its regional offices [Ref. 4: p. 9-5]. It is also suggested that as many audit staff personnel as possible should attend either or both of the DON-sponsored 40-hour ADP Security Courses [Ref. 4: p. D-1]. Any additional training for ADP audit staff members in the areas of ADP security or ADP security audit procedures would be most helpful in the development of a good ADP security audit staff.

What action can the newly formed audit staff undertake while they are receiving additional training? They should review their ADP system in order to best determine in their own minds if they feel that their system is secure. What must a secure system be able to do?

> The secure system must be able to identify all attempted violations--accidental or malicious. Any mismatch of user or terminal identification, password or lock word, or any unauthorized request for processing or data requires some reaction. At a minimum, the system should record the attempt in a log. [Ref. 20: p. 81]

When the audit staff understands the basic meaning of a secure system, they may then attempt to determine the auditability of their ADP system. A checklist that may be

used to determine the auditability of an ADP system is given below:

Auditability Checklist

1. Are adequate records kept of all attempts to access proprietary information?
2. Is a record kept of all authorized accesses that clearly identifies the data accessed, who accessed it, and when?
3. Is a periodic report of all authorized accesses to top-priority information or changes to the authorized access tables provided to management?
4. Is management provided with timely reports of unauthorized access attempts?
5. Does management use the provided reports?
6. Is the record-retention period adequate for these logs? [Ref. 20: p. 81]

Obtaining adequate professional training, establishing a common understanding of a secure system and determining the auditability of their particular ADP security system are three initial actions that must be considered by a new ADP audit staff.

A good internal audit program will contain continual professional training for its members and an active ongoing audit to continually establish the security of the ADP system.

A suggested audit cycle format is listed in Table VI [Ref. 20: p. 94]. This audit cycle is just a sample and would have to be modified depending on the size of staff, expertise of staff and the individual needs of the command.

TABLE VI

ESTIMATED AUDIT DAYS

Subject		Audit Days
Preaudit strategy and initial audit meeting		2
Security organization		½
Perimeter and after-hours security		4
Entrances	1/2	
Employee identification	1	
Nonpermanent employee control	1/2	
Key control	1/2	
Guard duties	1	
After-hours tour	1/3	
Information service functions (Approximately 2 hours per function)		3
Top-priority document control		2
New product security (2 days per unannounced product)		4
Trade secrets (2 days per trade secret)		4
Employee awareness		½
Destruction		½
Data security		6
Data processing organization	1/2	
Computer center access control	1/4	
Data-access control	3/4	
Tape and disk library	1/2	
Bulk transmission	1/4	
Remote computing	3	
System design	1/2	
Top-priority information	1/4	
Writing audit report and final meeting		3½
TOTAL		30

The main thing that should be understood is that your internal ADP audit program must be an ongoing endeavor that is conducted by well-trained professionals. The success of your internal ADP audit program will often determine your success with audits conducted by sources outside of your organization.

XII. SUMMARY

This paper is intended as a guide to be used by the NFC personnel in the development of a viable ADP security plan. An attempt has been made to combine the requirements established by OPNAVINST 5239.1A with selected information about ADP security from other readings and present them in a manner that might best assist NFC personnel in the development of an ADP security plan.

The importance of a staff being developed with its primary purpose being ADP security cannot be overemphasized. Since ADP security is a support function for the NFC, Cleveland, it should be realized that the creation of a staff with its primary purpose being ADP security will be a problem that must be confronted. The establishment of an ADP security staff and their professional training in ADP security is the first step toward the development of an ADP security plan. When a trained ADP security staff has been established and an initial draft made of a command ADP security plan, the ongoing awareness and training of all command personnel will make the plan a success. Chapters on the development of an ADP security training plan and ways to prepare for an ADP security audit have been included.

The elements that should be included in a comprehensive ADP security plan have each had a chapter devoted to them.

They include risk assessment, physical security, systems security and contingency planning. An additional chapter has been included to discuss the necessary managerial procedures needed for the implementation of an ADP security plan.

This paper used in conjunction with OPNAVINST 5239.1A should provide adequate guidance for the development of an initial ADP security plan for the NFC Cleveland. When the plan has been developed, its success will depend on the command personnel that must update and implement the plan.

APPENDIX A

SECURITY CHECKLIST ASSESSMENT

SECURITY CHECKLIST ASSESSMENT

Security/Management/Personnel	Yes	No	Partial
1. Is there a written overall ADP system security plan?	___	___	___
2. Does any type of internal audit effort exist to determine compliance with security procedures?	___	___	___
3. Have the resource impacts of site ADP security requirements been fully analyzed and identified?	___	___	___
4. Have ADP security resource requirements been entered into command programming and budget documents?	___	___	___
5. Do you have a formalized contingency plan?	___	___	___
6. Do your supervisors advise you of a possibly disgruntled employee?	___	___	___
7. Are all employees cleared to the highest level of data processed at the installation?	___	___	___
8. Do you recheck employees periodically?	___	___	___
9. Are security and operations personnel briefed on how to react to civil disturbances?	___	___	___
10. Have appropriate personnel been briefed on the destruction or safeguarding of classified material in the central computer facility in the event the facility must be evacuated?	___	___	___
11. Do you have people cross-trained to cover all functions?	___	___	___
12. Do your personnel know how to handle telephone bomb threats?	___	___	___

Building/Facility	Yes	No	Partial
1. Is the building structurally sound?	___	___	___
2. Is the building on solid foundation?	___	___	___
3. Is the building remote from any earthquake faults?	___	___	___
4. Are building and equipment properly grounded for lightning protection?	___	___	___
5. Is the computer/terminals housed in building(s) which is fire-resistant and constructed of non-combustible materials?			
6. Are there any high risk operations near by?	___	___	___
7. Is battery powered emergency lighting provided?	___	___	___
8. Are computers excluded from areas below grade?	___	___	___
9. Are drains installed on floor above to divert water accumulations away from all hardware?	___	___	___
10. Do you insist on the elimination of any overhead steam or water pipes except for sprinklers?	___	___	___
11. Do you have adequate drainage to provent water overhead from adjacent areas?	___	___	___
12. Do you have adequate drainage under the raised floor?	___	___	___
13. Are large plastic sheets available to cover equipment for quick emergency water protection?	___	___	___

Power Supply	Yes	No	Partial
1. Have you monitored your power source with recorders to identify electrical transients?	___	___	___
2. If your system requires motor generators, do you have backup?	___	___	___
3. Do you have a back-up power supply (diesel/elec. etc.)	___	___	___
4. Is backup power tested at regular intervals?	___	___	___
5. In the event of power failure do you have emergency lighting for removal of personnel?	___	___	___
6. Are cipher doors and fire alarm systems backed up with battery for removal of personnel?	___	___	___
7. Do you have emergency power off at all exits and within computer center?	___	___	___
8. Are emergency power offs protected from accidental activation?	___	___	___
9. Does the emergency power off also disable the environmental control system?	___	___	___

Environmental Supply	Yes	No	Partial
1. Is the environmental support system specifically dedicated to the computer center?	___	___	___
2. Do you have backup air conditioning capability?	___	___	___
3. Are air intakes:			
a) Covered with protective screening?	___	___	___
b) Located as to prevent intake of pollutants or other debris?	___	___	___
4. Is compressor remote from computer room?	___	___	___
5. Are duct linings noncombustible?	___	___	___
6. Are filters noncombustible?	___	___	___
7. Is air temperature and humidity recorded in computer environment?	___	___	___

Fire Protection	Yes	No	Partial
1. Is the computer housed in a building which is constructed of fire-resistant and noncombustible materials?	___	___	___
2. Is the computer room separated from adjacent areas by noncombustible fire-resistant partitions, walls, and doors?	___	___	___
3. Are flammable or otherwise dangerous activities prohibited from adjacent areas or areas above or below the computer room?	___	___	___
4. Are ceilings and support hardware (for hung ceilings) noncombustible?	___	___	___
5. Is raised flooring made of noncombustible material?	___	___	___
6. Are paper and other combustible supplies stored outside the computer area?	___	___	___
7. Are file tapes and disks stored outside the computer area?	___	___	___
8. Are smoke detectors installed:			
a) In ceiling?	___	___	___
b) Under raised floor?	___	___	___
c) In air-return ducts?	___	___	___
9. Do you test the smoke detection system on a scheduled basis?	___	___	___
10. Does smoke detection equipment shutdown air conditioning system?	___	___	___
11. Is the computer area protected by:			
a) Automatic carbon dioxide?	___	___	___
b) Halogenated agent?	___	___	___
c) Water?	___	___	___

Fire Protection	Yes	No	Partial
d) Wet pipe (releases water at a set temperature)?	___	___	___
e) Preaction (may sound an alarm and delay release of water)?	___	___	___
12. Are operators trained periodically in fire-fighting techniques and assigned individual responsibilities in case of fire?	___	___	___
13. Are portable fire extinguishers spread strategically around the area with location markers clearly visible over computer equipment?	___	___	___
14. Do you hold "fire drills," regularly?	___	___	___
15. Do you have enough fire alarm pull boxes within the computer areas and throughout the facility?	___	___	___
16. Does the alarm sound? a) Locally?	___	___	___
b) At watchman station?	___	___	___
c) At central station?	___	___	___
d) At fire or police headquarters?	___	___	___
17. Can emergency crews gain access to the installation without delay?	___	___	___
18. Do emergency crews respond in a timely fashion?	___	___	___
19. Do you clean under raised floor regularly?	___	___	___
20. Do you prevent accumulation of trash in the computer area?	___	___	___
21. Are paper and supplies stored outside computer room?	___	___	___

Fire Protection	Yes	No	Partial
22. Are tapes and disks stored outside computer room?	___	___	___
23. Do you have adequate supply of firefighting water available?	___	___	___
24. Are emergency power shutdown controls easily accessible at points of exit?	___	___	___
25. Does emergency power shutdown include air conditioning system?	___	___	___
26. Do you have battery-powered emergency lighting throughout the computer area?	___	___	___
27. If access is via an electronically controlled system, can it be operated by standby battery power?	___	___	___

Physical Access	Yes	No	Partial
1. Are guards posted at entrances.	___	___	___
2. Do you have a photo badge system for positive identification of employees?	___	___	___
3. Do you utilize keys, cipher locks, and other security devices to control access?	___	___	___
a) Are keys, ciphers, etc. changed at regular intervals and after termination of an employee?	___	___	___
4. Can an individual gain access without the knowledge of a security guard or another employee?	___	___	___
5. Is access to the computer area restricted to selected personnel?	___	___	___
6. Do all personnel having unescorted access to the system possess a clearance/special access authorization equal to or higher than the highest classification and all categories being processed?	___	___	___
7. Are all computer operators and system programming personnel cleared for the highest level and most restrictive category of classified information in the system?	___	___	___
8. Is the central computer facility manned by at least two appropriately cleared personnel at all times?	___	___	___
9. Do you have a visitor control procedure?	___	___	___
10. Are escort procedures established for controlling visitors?	___	___	___

Physical Access	Yes	No	Partial
11. Is in-house service personnel traffic			
a) Controlled in vital areas?	___	___	___
b) Supervised?	___	___	___
12. Is a list prepared for authorized vendor service personnel?	___	___	___
13. Is positive identification required for vendor service personnel?	___	___	___
14. Are vendor service personnel supervised while on premises?	___	___	___
15. Are vendor employee background checks verified?	___	___	___
16. Are dismissed employees of computer environment removed immediately, their admission badges picked up, the necessary guard personnel notified, and their permissions to the system deleted immediately?	___	___	___
17. Do you perform background checks on employees periodically?	___	___	___

Data Protection	Yes	No	Partial
1. Are files (tape, disk, or card) kept in an area other than the computer room?			
a) Is this area fire-protected?	___	___	___
b) Is access specifically controlled?	___	___	___
2. Is your tape library located in an area secure from explosion or other dangers?	___	___	___
3. Are all data files maintained within and under the control of the computer complex rather than the user?	___	___	___
4. Do you maintain duplicates of all programs and data files?	___	___	___
5. Do you have a current inventory of such files?	___	___	___
6. Are the duplicate files stored in a separate building from the originals?	___	___	___
7. Do you maintain duplicates of all documentation?	___	___	___
8. Are the documentation duplicates stored in a separate building?	___	___	___
9. Do you review your documentation backup periodically to ensure its current applicability?	___	___	___
10. Do you maintain any type of backup of source data for programs under development?	___	___	___
11. Is the duplicate filed in a separate building from the original?	___	___	___
12. Have you held a "dry run" in the past 3 months to test the ease and accuracy of your file backup system?	___	___	___
13. Are changes in programs and documentation coordinated and approved by the cognizant areas:	___	___	___

Data Protection	Yes	No	Partial
14. Are changes made only to a reproduced version of the original program file with the original left intact?	—	—	—
15. Does your tape and disk accountability procedure cover:			
a) Frequency of use?	—	—	—
b) Frequency of cleaning?	—	—	—
c) Authorized user?	—	—	—
16. Are magnetic tapes and disks filed in an orderly manner?	—	—	—
17. Are tapes stored vertically?	—	—	—
18. Are tapes kept in their containers except when in use?	—	—	—
19. Are tape heads cleaned every shift?	—	—	—
20. Have you considered magnetic detection equipment to preclude the presence of a magnet near your tapes and disks?	—	—	—
21. Do you provide similar protection for your tape files while they are in transit to a backup site, etc.?	—	—	—
22. Do you use storage vaults specifically designed for magnetic media for critical tape files?	—	—	—

Data Protection	Yes	No	Partial
23. Do you have documentation standards which include:			
a) Logic or flow charts?	___	___	___
b) Current listing?	___	___	___
c) Input and output forms?	___	___	___
d) Output samples?	___	___	___
e) Copies of test data?	___	___	___
f) Adequate explanation of codes, tables calculations, etc.?	___	___	___
g) Explanation of error messages?	___	___	___

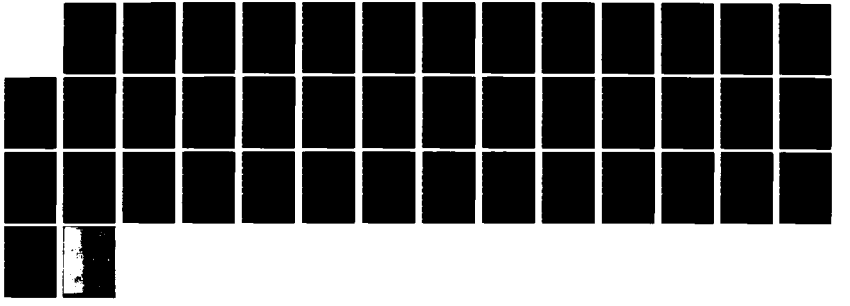
Operating System	Yes	No	Partial
1. Are security-override procedures classified at the highest level and the use of override closely monitored?	___	___	___
2. Is program debugging of the security system monitored and controlled?	___	___	___
3. Are <u>all</u> modifications to the operating system monitored by the security office?	___	___	___
4. Do you "utilize" passwords to identify a specific terminal and a specific user?	___	___	___
5. Is the password combined with physical keys or access badges?	___	___	___
6. Are passwords changed frequently?	___	___	___
7. Is the password protection system really tamperproof?	___	___	___
8. Does the system software restrict a given individual to specific data files only?	___	___	___
9. Is access to the "keyword" and "lockword" files restricted?	___	___	___
10. Are remote terminals available only to selected individuals?	___	___	___
11. Is access to terminal controlled by: a) Locked doors?	___	___	___
b) Posted guards?	___	___	___
12. Is the location of the terminal such that each user's privacy is ensured?	___	___	___
13. Is a monitor program maintained to record all access attempts to secure or sensitive files?	___	___	___

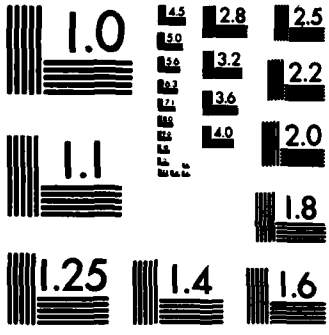
Operating System	Yes	No	Partial
14. Are dial-up terminals disabled from connection to the system during periods of classified processing?	___	___	___
15. Do you use a software security routine to monitor illegal sign-on or access attempts?	___	___	___
a) Does this routine notify the operator via the console?	___	___	___
b) Does this routine provide a hardcopy record at the end of each shift/day?	___	___	___

Software Security	Yes	No	Partial
1. Have you restricted access to the essential programs and software systems on a need-to-know basis in the prime and backup areas?	___	___	___
2. Do you employ keyword or password protection?	___	___	___
3. Are the essential programs, software systems, and associated documentation in your Program Library located in a locked vault or secure area?	___	___	___
4. Have you provided backup files at a secondary location for both the programs and the associated documentation?	___	___	___
5. Are programming changes and maintenance well controlled and documented?	___	___	___
6. Do you restrict terminal users to higher level languages to prevent their access to machine language coding?	___	___	___
7. Do you use a software security routine to monitor attempts to access sensitive files by unauthorized users?	___	___	___
a) Does this routine notify the operator via the on-line console?	___	___	___
b) Does this routine provide a record of all such attempts via a printout at day's end?	___	___	___
8. Can your own software systems technologists be depended upon not to circumvent the normal access procedures by use of a special coding thus violating the integrity of the system?	___	___	___
9. Is a record of all operating system modifications maintained until at least the next sofware release?	___	___	___

AD-A127 244 A GUIDE FOR DEVELOPING AN ADP SECURITY PLAN FOR NAVY FINANCE CENTER CLEVELAND OHIO(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA D E BARBER ET AL. DEC 82 3/3

UNCLASSIFIED F/G 9/2 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Software Security	Yes	No	Partial
1. Have you restricted access to the essential programs and software systems on a need-to-know basis in the prime and backup areas?	___	___	___
2. Do you employ keyword or password protection?	___	___	___
3. Are the essential programs, software systems, and associated documentation in your Program Library located in a locked vault or secure area?	___	___	___
4. Have you provided backup files at a secondary location for both the programs and the associated documentation?	___	___	___
5. Are programming changes and maintenance well controlled and documented?	___	___	___
6. Do you restrict terminal users to higher level languages to prevent their access to machine language coding?	___	___	___
7. Do you use a software security routine to monitor attempts to access sensitive files by unauthorized users?	___	___	___
a) Does this routine notify the operator via the on-line console?	___	___	___
b) Does this routine provide a record of all such attempts via a printout at day's end?	___	___	___
8. Can your own software systems technologists be depended upon not to circumvent the normal access procedures by use of a special coding thus violating the integrity of the system?	___	___	___
9. Is a record of all operating system modifications maintained until at least the next sofware release?	___	___	___

Audit Controls		Yes	No	Partial
1.	Are program changes adequately controlled?	___	___	___
2.	Is the log-on procedure secure?	___	___	___
3.	Are all options of all programs really tested?	___	___	___
4.	Do error reporting and adequate follow-up procedures exist?	___	___	___
5.	Is input data verified against an authorized user list?	___	___	___
6.	Is output data verified against an authorized user list?	___	___	___
7.	Do you spot-check output frequency for possible misuse of the system?	___	___	___
8.	Do you verify all periods of down time as to length and reason?	___	___	___
9.	Has the facility been evaluated in accordance with applicable TEMPEST procedures to determine risk?	___	___	___
10.	Has all installed ADPE been TEMPEST tested?	___	___	___
11.	Are all changes, repairs, and modifications to TEMPEST modified ADPE controlled so that equipment emanations characteristics are not altered?	___	___	___
12.	Is magnetic detection equipment used?	___	___	___

APPENDIX B

RISK ASSESSMENT DOCUMENTATION

B.1. SAMPLE RISK ASSESSMENT TEAM CHARTER

SAMPLE RISK ASSESSMENT TEAM CHARTER

Canc frp: Date
NARDACNORFOLKNOTE 5450
Ser:

NARDAC NORFOLK NOTICE 5450

From: Commanding Officer, Navy Regional Data Automation Center, Norfolk

Subj: Risk Assessment Team Charter

Ref: (a) OPNAVINST 5239.1A

Encl: (1) Work Plan and Schedule

1. Background

a. Reference (a) requires all Navy automatic data processing (ADP) activities to perform a risk assessment to determine the potential and actual threats and vulnerabilities which could cause disruptions in service or compromise of information. Reference (a) states that a risk assessment is to be performed whenever major changes occur in hardware or operating systems software, or no less frequently than once every five years. Additionally, reference (a) outlines those action items to be accomplished when conducting a comprehensive risk assessment.

b. The major function of this risk assessment is to provide quantitative information upon which decisions regarding the selection and implementation of countermeasures can be based. Secondary functions include the documentation of assets and the assignment of priorities to work loads.

2. Objectives. The objectives of the NARDAC Norfolk risk assessment are to:

a. Determine the current security posture of the facility

b. Recommend appropriate countermeasures for implementation

FIGURE H-2 (Page 1 of 5)

SAMPLE RISK ASSESSMENT TEAM CHARTER

3. Risk Assessment Team Charter

a. Risk Assessment Team Leader

(1) Code 30X is designated as the team leader for the NARDAC Norfolk risk assessment project with the authority to:

(a) Report directly to the Executive Officer on project matters

(b) Make task assignments to primary and secondary team members

(c) Request information from all sources within NARDAC Norfolk

(d) Establish milestones within the framework of the risk assessment project

(2) It is the responsibility of the team leader to:

(a) Coordinate the activities of team members to minimize duplication of effort

(b) Provide periodic reports to the Executive Officer regarding the status of the project

(c) Make recommendations based upon the risk assessment to correct or improve deficiencies

(d) Consolidate independent studies into a final report

b. Risk Assessment Team Members

(1) The primary team will consist of Codes 30X, 50X, and 23.

(2) Codes 07, 09L, and 40 will supply secondary team representatives by name by 5 June 1981 to participate on an as required basis.

(3) Primary team members for the duration of the project have the authority to:

FIGURE H-2 (Page 2 of 5)

SAMPLE RISK ASSESSMENT TEAM CHARTER

(a) Review all internal command and operating procedures and documentation

(b) Conduct physical inspections

(c) Hold interviews with NARDAC personnel

(d) Make privileged mode computer runs

(e) Establish parameters for accomplishing the project

(4) The responsibilities of the Risk Assessment Team include the investigation and documentation of all items relating to the ADP security of NARDAC Norfolk and the conducting of a risk assessment in accordance with Appendix E of reference (a).

4. Deliverable Products. Upon completion of this project, the Risk Assessment Team will provide the following items:

a. Prioritized Workload Chart

b. Computer/Peripheral Inventory

c. Program Inventory

d. Data File Inventory

e. Annual Loss Expectancy (ALE) Computations

f. Threat and Vulnerability List

g. Recommendations for Corrective Action

h. Plant Facilities Inventory

5. Commitment. Personnel from all departments are to provide the cooperation and assistance required by the Risk Assessment Team. It is the intent of this project to identify problem areas so corrective action can be taken, rather than attribute deficiencies to individuals or departments. It is the command's position that ADP security requires a commitment by every individual and will be enthusiastically supported by all.

FIGURE H-2 (Page 3 of 5)

SAMPLE RISK ASSESSMENT TEAM CHARTER

6. Action. Effective immediately the designated team leader will form the Risk Assessment Team as specified above and proceed in accordance with the work plan and schedule provided as enclosure (1).

7. Cancellation Contingency. This notice is cancelled upon receipt of the next issuance.

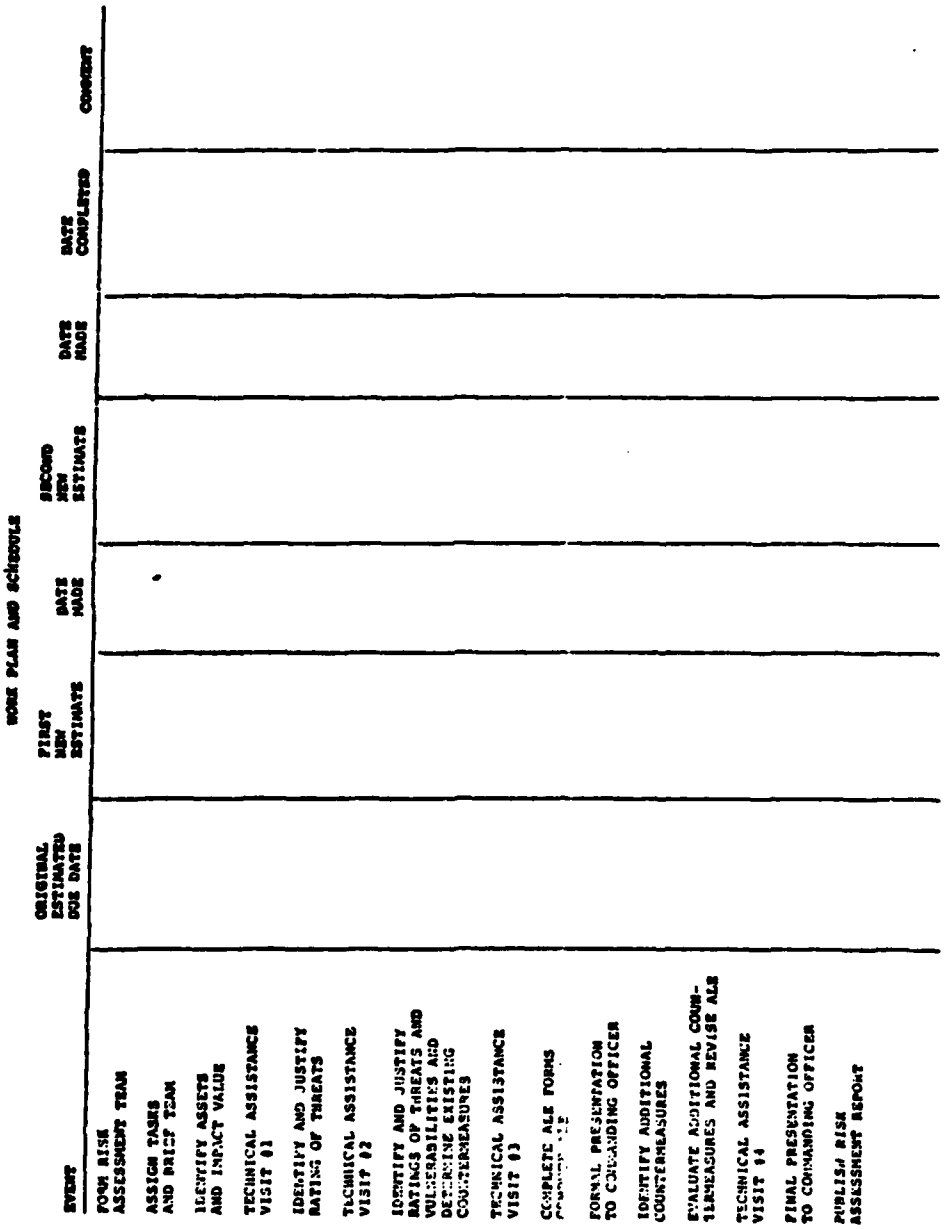
Commanding Officer

Signature

Distribution:
OOT
09
09L
07
20
30
40
50

FIGURE H-2 (Page 4 of 5)

SAMPLE RISK ASSESSMENT TEAM CHARTER



Enclosure (1)

FIGURE H-2 (Page 5 of 5)

B.2. SAMPLE FORMAT ADP SECURITY SURVEY

OPNAVINST 5238.1A

AUG 3 1982

SAMPLE FORMAT
ADP SECURITY SURVEY

SECTION I. Basic Data. (Applies to all ADP systems, networks, and OISs)

1. System Identification: _____

( ) Office Information System

( ) ADP System

( ) Network

2. System Description: (List all components, main frames, peripherals, communications processors, encryption devices, remote devices, network and remote interfaces, etc.)

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

FIGURE E-1 (Page 1 of 10)

E-18

SAMPLE FORMAT
ADP SECURITY SURVEY

3. Equipment Location: _____

4. System Operations Contact for Security:

Name: _____ Code: _____

Bldg: _____ Room: _____ Phone: _____

5. Types of Data Processed and Security Modes of Operation

TYPE OF DATA	PERCENT OF PROCESSING TIME	SECURITY MODE OF OPERATION*
Level I		
SCI		
SIOP-ESI		
TOP SECRET		
SECRET		
CONFIDENTIAL		
Level II		
Privacy Act		
For Official Use Only		
Financial		
Sensitive Management		
Proprietary		
Privileged		
Level III		
TOTAL	100%	

(Note: Applicable security modes are: Compartmented, Controlled, Dedicated, System High, Multilevel, Limited Access, as defined in Appendix A of this manual.)

FIGURE E-1 (Page 2 of 10)

SAMPLE FORMAT
ADP SECURITY SURVEY

6. Operating System and Standard Applications Software Identifications:

_____

_____

_____

7. Scope of System: (Check all that apply.)

( ) Stand-alone and single controlled area (single CPU with single workstation).

( ) Shared logic and single controlled area (single CPU with multiple workstations).

( ) Shared logic and more than one controlled area (single CPU with multiple workstations).

( ) Multiple processors and single controlled area (multiple CPUs).

( ) Multiple processors and more than one controlled area (multiple CPUs).

( ) Used with a remote computer _____ percent of time.

( ) Other: _____

8. Total Value of System: $ _____ (Dollar value impact of loss and cost to replace)

A. Equipment: $ _____

B. Software: $ _____

C. Data: $ _____
(Note: Dollar values in Table E-2 can be used as a guideline for computing value of data files.)

FIGURE E-1 (Page 3 of 10)

SAMPLE FORMAT
ADP SECURITY SURVEY

9. Mission Relatedness

A. Primary Function(s) of the System or Network:

_____

_____

_____

B. Contingency Plan Requirement:

( ) Plan is in existence. Date of plan is _____

( ) Plan is being developed. Estimated completion date is _____.

( ) Plan is not required because loss of processing capability for a reasonable period of time would not adversely affect mission. (For example, 2, 4, 8 hours, 2 days, etc. depending on the criticality of the ADP function.) Provide justification.

Section II. Site Security Profile and Minimum Requirements for Environmental and Physical Security. (Applies to all ADP systems, networks, and OISs.)

1. Vulnerability: Temperature or Humidity Outside Normal Range.

Operating Countermeasures: (Check all that apply.)

( ) Adequate heating and controls
( ) Adequate cooling and controls
( ) Only designated personnel operate controls
( ) Functioning temperature and humidity recorder
( ) Functioning temperature/humidity warning system
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate ( ) Low

FIGURE E-1 (Page 4 of 10)

SAMPLE FORMAT
ADP SECURITY SURVEY

2. Vulnerability: Inadequate Lighting or Electrical Service.

Operating Countermeasures: (Check all that apply.)

( ) Adequate primary lighting
( ) Adequate emergency lighting
( ) Adequate periodic checks of emergency lighting
( ) Adequate primary power and outlets
( ) Functioning power filters or voltage regulators
( ) Available backup power
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate ( ) Low

3. Vulnerability: Improper Housekeeping.

Operating Countermeasures: (Check all that apply.)

( ) Routine cleaning schedule is adhered to
( ) Cleaning personnel are trained in computer room *procedures*
( ) An ADP facility representative is present during cleaning
( ) Dust contributors are not permitted in equipment areas (outer coats, throw rugs, drapes, venetian blinds, etc.)
( ) Air-conditioning filters are cleaned/replaced regularly
( ) Floors are polished with non-flake wax using proper buffer materials or properly damp-mopped
( ) Carpet areas are vacuumed frequently and anti-static spray is used regularly
( ) Smoking, eating, and drinking are not permitted in equipment areas
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate ( ) Low

FIGURE E-1 (Page 5 of 10)

SAMPLE FORMAT
ADP SECURITY SURVEY

4. Threat: Water Damage.

Operating Countermeasures: (Check all that apply.)

( ) Water/steam pipes are not located above equipment
( ) Water/steam pipes are inspected at regular intervals
( ) Functioning humidity warning system
( ) Dry-pipe sprinkler system
( ) Raised floor
( ) Plastic sheets available to cover susceptible equipment
( ) Water detection devices
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate ( ) Low

5. Threat: Fire.

Operating Countermeasures: (Check all that apply.)

( ) Up-to-date fire bill posted
( ) Periodic fire drills
( ) Training--fire prevention methods
( ) Training--emergency power down procedures
( ) Trainng--knowledge of fire detection system
( ) Training--use of fire extinguishers
( ) Training--use of fire alarm system
( ) Training--evacuation plan
( ) Training--individual responsibilities in case of fire
( ) Functioning emergency power-off switches
( ) Sprinkler system installed
( ) Halon system installed
( ) Carbon dioxide fire extinguishers installed
( ) Smoke/heat detectors installed
( ) Functioning fire alarm system
( ) Emergency exits clearly marked
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate ( ) Low

FIGURE E-1 (Page 6 of 10)

SAMPLE FORMAT
ADP SECURITY SURVEY

6. Vulnerability: Unauthorized Physical Access.

Operating Countermeasures: (Check all that apply.)

( ) Perimeter fence
( ) Security guards
( ) Building secured outside of normal working hours
( ) Area alarms (motion detectors, open door detectors, perimeter penetration detectors)
( ) Authorized access list
( ) Cypher door lock
( ) Combination door lock
( ) Recognition of authorized personnel
( ) Closed circuit television
( ) Administrative procedures
( ) Physical isolation/protection
( ) High employee morale
( ) Close supervision of employees
( ) Indoctrination of personnel in security awareness
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate ( ) Low

SECTION III. Current status of accreditation support documentation. (Applies to all ADP activities and networks which will be authorized to handle Level I or Level II data.)

1. All ADP activities and networks which will be authorized to handle Level I or II data must either be accredited or be granted interim authority to operate pending accreditation. Accreditation is based on supporting documentation including a risk assessment. This section provides a statement of the current status of the accreditation support documentation. (Check all that apply.)

FIGURE E-1 (PAGE 7 of 10)

SAMPLE FORMAT
ADP SECURITY SURVEY

_____ In existence
_____ Being developed
_____ Required but no action taken
_____ Not required

( ) ( ) ( ) ( ) Security Operating Procedures Handbook
( ) ( ) ( ) ( ) Line diagrams showing interconnection of components and physical layout
( ) ( ) ( ) ( ) Description of countermeasures in place
( ) ( ) ( ) ( ) Copies of previous accreditation or interim authority to operate
( ) ( ) ( ) ( ) TEMPEST accreditation request
( ) ( ) ( ) ( ) TEMPEST accreditation test results
( ) ( ) ( ) ( ) Physical accreditation
( ) ( ) ( ) ( ) ST&E Test Plan
( ) ( ) ( ) ( ) Contingency Plan
( ) ( ) ( ) ( ) Contingency Plan test results
( ) ( ) ( ) ( ) Formal Risk Assessment
( ) ( ) ( ) ( ) Other (specify): _____

SECTION IV. Countermeasure Documentation for Office Information Systems. (Applies to all OISs which will be authorized to handle Level I or Level II.)

1. OISs Handling Level II Data. (Check all that apply.)

( ) The OIS will be authorized to handle Level II data. A list of the operating countermeasures is attached. These countermeasures provide proper data protection and audit trails.

( ) The OIS is a shared logic system with more than one simultaneous user not having need-to-know for all data within the system. Password protection or other equivalent countermeasures are employed for system access and for individual file access.

( ) The OIS Security Operating Procedures have been documented and approved.

FIGURE E-1 (Page 8 of 10)

SAMPLE FORMAT
ADP SECURITY SURVEY

2. OISs handling Level I Data. (Check all that apply.)

( ) The OIS will be authorized to handle Level I data under a system high or dedicated mode of operation. A list of the operating countermeasures is attached. These countermeasures satisfy security requirements.

( ) TEMPEST accreditation has been requested. Request date _____.

( ) TEMPEST accreditation has been received. Accreditation date _____.

( ) The OIS Security Operating Procedures have been documented and approved.

SECTION V. Survey Data. (Applies to all ADP systems, networks, or OISs.)

1. Current Status: (Check all that apply.)

( ) Operating under accreditation for processing Level _____ data in _____ security mode of operation. Accreditation granted by _____. Dated _____. (Attach a copy of statement of accreditation.)

( ) Operating under interim authority for processing Level _____ data in _____ security mode of operation. Interim authority granted by _____. Dated _____. Expires _____. (Attach a copy of interim authority to operate.)

2. Survey Prepared By:

Name:_____ Code:_____

Bldg:_____ Room: _____ Phone:_____

FIGURE E-1 (Page 9 of 10)

SAMPLE FORMAT
ADP SECURITY SURVEY

To the best of my knowledge, the information provided in this survey and the attached documentation is complete and accurate.

Signature _____ Date _____

(Provide a list of all survey team members.)

FIGURE E-1 (Page 10 of 10)

E-27

B.3. EXAMPLES OF ASSETS

EXAMPLES OF ASSETS

HARDWARE

- Central Machine
  - CPU
  - Main memory
  - I/O channels
  - Operator's console
- Storage Medium
  - Magnetic media
    - Disk pack
    - Magnetic tapes
    - Diskettes (floppies)
    - Cassettes
    - Drums
  - Nonmagnetic media
    - Punched cards
    - Paper tape
    - Paper printout
- Special Interface Equipment
  - Network front ends
  - Data base machines
  - Intelligent controllers
- I/O Devices
  - User directed I/O devices
    - Printer
    - Card reader
    - Card punch
    - Paper tape reader
    - Terminals - local and remote
  - Storage I/O device
    - Disk drives
    - Tape drives

SOFTWARE

- Operating System
- Programs
  - Application
  - Standard application/operating programs
  - System utilities
  - Test programs
  - Communications

PHYSICAL

- Environmental Systems
  - Air-conditioning
  - Power
  - Water
  - Lighting
- Building
- Computer Facility
  - Computer room
  - Data reception
  - Tape and disk library
  - Customer engineer room
  - I/O area
  - Data preparation area
  - Physical plant room
- Backup Equipment
  - Auxiliary power
  - Auxiliary environmental controls
  - Auxiliary supplies
- Supplies
  - Magnetic media
  - Paper
  - Ribbons

PERSONNEL

- Computer Personnel
  - Supervisory personnel
  - Systems analysts
  - Programmers
    - Applications programmers
    - Systems programmers
  - Operators
  - Librarian
  - Security Officer
  - Maintenance personnel
  - Temporary employees and consultants
  - System evaluators and auditors
  - Clerical personnel
- Building Personnel
  - Janitors
  - Guards
  - Facility engineers
- Installation Management

ADMINISTRATIVE

- Documentation
  - Software
  - Hardware
  - File
  - Program
  - JCL
  - System
- Operations
  - Schedules
  - Operating guidelines and manuals
  - Audit documents
- Procedures
  - Emergency plans
  - Security procedures
  - I/O procedures
  - Integrity controls
- Inventory Records
- Operational Procedures
  - Vital records
  - Priority-run schedule
  - Production procedures

DATA

- Classified
- Operations
- Tactical
- Planning
- Financial
- Statistical
- Personal
- Logistic
- Other

COMMUNICATIONS

- Communications Equipment
  - Communications lines
  - Communications processors
  - Multiplexors
  - Switching devices
  - Telephones
  - Modems
  - Cables

B.4. ASSET VALUATION WORKSHEET

OPNAVINST 5239.1A

AUG 3 1982

SAMPLE

ASSET VALUATION WORKSHEET

1. ASSET NAME

System A Operating System and Support Programs

2. ASSET DESCRIPTION AND JUSTIFICATION OF IMPACT VALUE RATINGS ASSIGNED.

Operating system and compiler support software for the System 'A' timesharing system.

Impact of modification was determined to be negligible, except in those cases where modification would result in denial of service. Those figures were included under denial of service.

Destruction was based on total destruction of all software and on-site backup tapes. These figures include denial of service caused by destruction.

Forty hours is required for delivery and check out of replacement O/S software. 75 users denied service at $12/hour; plus 6 system programmers at $14/hour for 16 hours; plus 3 data processing technicians at $8/hour for 36 hours. Total for the operating system = $39,936.

Sixty users denied use of the compiler at $12/hour for 24 hours; plus 1 system programmer at $14/hour for 8 hours. Total for the compiler support software = $1,832.

Reconstruction of compiler support data based on 618 hours to re-enter data at $8/hour. Total for compiler support data = $4,944.

Disclosure - N/A.

Denial of service was based on the number of users denied service for an average service outage.

Operating system: 35 users at $12/hour for 1 hour = $420.

Compiler support software: 35 users at $12/hour for 6 hours = $210.

Compiler support data - N/A.

3. IMPACT VALUE RATING BY IMPACT AREA

N/A MODIFICATION | 3 DESTRUCTION | N/A DISCLOSURE | 3 DENIAL OF SERVICE

OPNAV 5239/9 (8-82)

B.5. THREAT AND VULNERABILITY WORKSHEET

OPNAVINST 5239.1A

AUG 3 1982

SAMPLE

THREAT AND VULNERABILITY EVALUATION WORKSHEET

1. THREAT NAME

Alteration of Software

2. DESCRIPTION, EXAMPLES, AND JUSTIFICATION BASED ON EXISTING COUNTERMEASURES AND VULNERABILITIES.

The ADP system or application software may be altered in an unauthorized manner. Software may be modified or destroyed, adversely affecting the data processed. Software alterations may result in program or system failure and denial of service to users.

Payroll and inventory control program alterations could result in monetary loss. Disclosure of the software itself is not a threat, but software changes could affect the data being processed, resulting in modification or disclosure of data.

There have been five incidents in the last six months where unauthorized software patches have crashed the system for periods up to a day. File maintenance software failed twice erasing the master data base. Reconstruction required 6½ hours. Default options on the application software were misprogrammed resulting in erroneous processing. Software generating control totals failed causing reruns. The program linkage control table software failed, thus preventing authorized programs from accessing required software modules. Down time amounted to 6 hours.

There are few audit trail features on the system. Configuration control procedures have not been formally documented. A password system is used, but passwords are infrequently changed and often commonly known or readily available. A large number of personnel have virtually unlimited access to the system. Users can access the system 24 hours a day. Software documentation does not keep pace with program changes.

3. SUCCESSFUL ATTACK FREQUENCY RATING BY IMPACT AREA.

[2] MODIFICATION [3] DESTRUCTION [2] DISCLOSURE [4] DENIAL OF SERVICE

OPNAV 5239/8 (2-82)

TABLE E-4

THREATS AND THEIR IMPACTS*

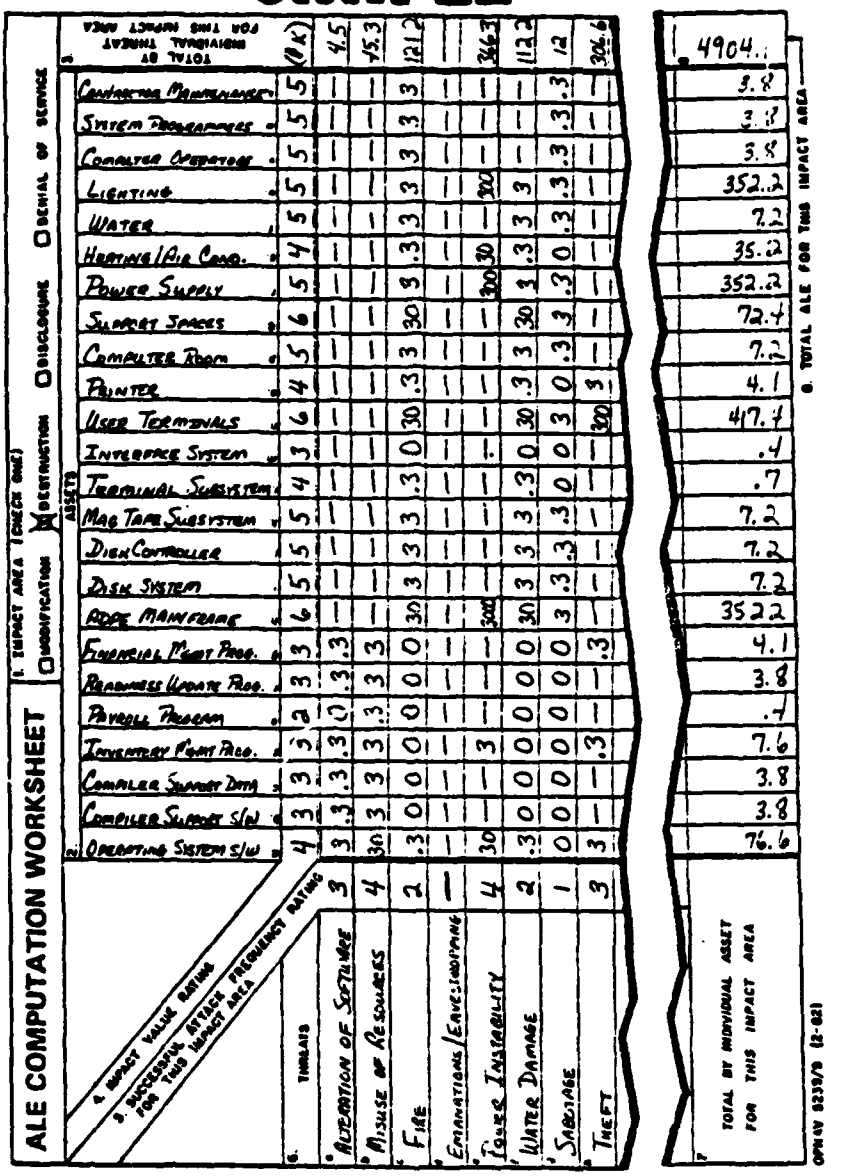
THREATS	IMPACT AREAS			
	Destruction	Disclosure	Modification	Denial of Service
Emanations/Eavesdroppng	No	Yes	No	No
Emanations (Interference)	Yes	No	Yes	Yes
Alteration of Software	Yes	Yes	Yes	Yes
Alteration/Failure of Hardware	Yes	Yes	Yes	Yes
Unintentional Operator Error	Yes	Yes	Yes	Yes
Unintentional Data Entry Error	Yes	Yes	Yes	Yes
Unintentional System Programmer Error	Yes	Yes	Yes	Yes
Unintentional Disclosure	No	Yes	No	No
Misuse of Computer Resources	Yes	Yes	Yes	Yes
Power Instability	Yes	No	Yes	Yes
Telecommunications Failure	No	No	No	Yes
Environmental Control Failure	No	No	No	Yes
Natural Disaster	Yes	No	No	Yes
Water Damage (Internal/External)	Yes	No	No	Yes
Fire (Internal/External)	Yes	No	No	Yes
Enemy Overrun/Civil Disorder	Yes	Yes	No	Yes

* Additional threats and impacts may be determined by the Risk Assessment Team.

B.7. ALE COMPUTATION WORKSHEET

OPNAVINST 5239.1A
AUG 3 1982

SAMPLE



B.8. ADDITIONAL COUNTERMEASURE EVALUATION WORKSHEET

OPNAVINST 5239.1A
AUG 3 1982

SAMPLE

ADDITIONAL COUNTERMEASURE EVALUATION WORKSHEET

1 COUNTERMEASURE NAME	2 ANNUAL COST
Audit Trail & Daily Review by ADPSSO	$26,000

3 DESCRIPTION

Review system software ($15,000), develop software controls ($5,000), and degradation of system operation with controls in place and system activity data reviewed daily by ADPSSO ($16,000 annually). Cost amortized over 5 years = $26,000. Develop software controls to capture system activity data (user name, log on/off time, terminal used, files requested, type of access, output generated). ADPSSO review daily to check for unusual user activity in the system.

4 THREATS AFFECTED BY THIS COUNTERMEASURE	5 ALE (a) CURRENT	5 ALE (b) PROJECTED	6 ALE SAVINGS
Alteration of Software	90.3K	4.5K	85.8K
Misuse of Resources	128.6K	12.6K	116K

7 RETURN ON INVESTMENT	8 TOTAL ANNUAL SAVINGS
7.8:1	201.8K

9 OVERLAPPING ADDITIONAL COUNTERMEASURES
Software Checksums
Improved Password Procedures
Modify Operating System to Permit Terminal Lockout after a Specified Number of Unsuccessful Log on Attempts
Improved Configuration Control Procedures

OPNAV 5239/10 (2-82)

B.9. ADDITIONAL COUNTERMEASURES SUMMARY LISTING

OPNAVINST 5239.1A
AUG 3 1982

SAMPLE

ADDITIONAL COUNTERMEASURES SUMMARY LISTING

1. ROI		2. ANNUAL COST	3. ALE SAVINGS		4. COUNTERMEASURE	5. MANDATORY REQUIREMENT
a. ORIGINAL	b. ADJUSTED		c. ORIGINAL	d. ADJUSTED		
7.8		26K	201.8K		AUDIT TRAIL & DAILY REVIEW BY ADPSO	
6.1	5.2	6K	36.6K	31.2K	MODIFY OPERATING SYSTEM TO PERMIT TERMINAL LOCKOUT	
5.9	3.2	1.3K	7.7K	4.2K	SOFTWARE CHECKSUMS	
4.3	1.3	3K	12.9K	3.9K	IMPROVED PASSWORD PROCEDURES	
1.5	1.1	3K	4.5K	3.3K	IMPROVED CONFIGURATION CONTROL PROCEDURES	
1.1	.4*	68K	74.8K	27.2K	TWO PERSON CONTROL * NOT RECOMMENDED; ADJUSTED ROI LESS THAN ONE.	

B.10. RISK ASSESSMENT MATRIX

OPNAVINST 5239.1A
AUG 3 1982

SAMPLE

RISK ASSESSMENT MATRIX

THREAT	SYSTEM SOFTWARE $ 700K		COMM EQUIP $ 500K		PHYSICAL FACILITY $ 1,200K		MAIN FRAME ADPE $ 500K		PERIPHERAL ADPE $ 500K		FINANCIAL MGMT PROGRAM $ 35K		UPDATE PROGRAM $ 2K		TOTAL ALE BY INDIVIDUAL THREAT
EMANATIONS	L	2.1K	H	165K	-	—	L	1.5K	M	16.5K	-	—	-	—	185.1K
MISUSE OF RESOURCES	M	23.1K	M	16.5K	-	—	M	16.5K	M	16.5K	L	.1K	L	0	72.7K
COMM FAILURE	L	2.1K	M	16.5K	-	—	M	16.5K	M	16.5K	L	.1K	L	0	51.7K
ALTERATION of SOFTWARE	L	2.1K	L	1.5K	-	—	-	—	-	—	H	1.2K	H	.7K	5.5K
FIRE	-	—	L	1.5K	L	3.6K	L	1.5K	L	1.5K	-	—	-	—	8.1K
POWER INSTABILITY	-	—	M	16.5K	L	3.6K	M	16.5K	M	16.5K	-	—	-	—	53.1K
THEFT	-	—	L	1.5K	-	—	-	—	-	—	-	—	-	—	1.5K
WATER DAMAGE	-	—	M	16.5K	M	39.4K	M	16.5K	M	16.5K	-	—	-	—	89.1K
SABOTAGE	L	2.1K	L	1.5K	L	3.6K	L	1.5K	L	1.5K	L	.1K	L	0	10.3K

TOTAL ALE BY INDIVIDUAL ASSET	41K	329.6K	65.5K	91.7K	111.2K	2.1K	1K	641.9K

B.11. ADDITIONAL COUNTERMEASURES SELECTION WORKSHEET

OPNAVINST 5239.1A

AUG 3 1982

SAMPLE

ADDITIONAL COUNTERMEASURES SELECTION WORKSHEET

a. ADDITIONAL COUNTERMEASURES	b. THREATS PAIRED	c. ORIGINAL ALE	d. REVISED ALE	e. ANNUAL SAVINGS	f. ANNUAL COST OF ADDITIONAL COUNTERMEASURES	g. RETURN ON INVESTMENT	h. ADDITIONAL COUNTERMEASURES PRIORITIES
1 AUDIT TRAIL & DAILY REVIEW BY ADPSO	ALTER S/W	5.5K	3.7K	1.8K			
	MISUSE	72.7K	6.6K	66.1K			
	ANNUAL SAVINGS SUBTOTAL			67.9K	12K	5.7:1	2
2 MODIFY TERMINALS TO PROVIDE UNIQUE ID FEATURE	COMM FAIL	51.7K	6.6K	45.1K			
	ANNUAL SAVINGS SUBTOTAL			45.1K	1.6K	28.2:1	1
3 DEDICATED ALTERNATE ROUTING LINES	COMM FAIL	51.7K	6.6K	45.1K			
	ANNUAL SAVINGS SUBTOTAL			45.1K	50K	0.9:1	NOT RECOMMENDED
4							

APPENDIX C

GUIDELINES FOR DESIGNATING POSITIONS ASSOCIATED WITH FEDERAL COMPUTER SYSTEMS

A-1. COVERAGE

This appendix provides specific criteria and amplifying guidance for determining the category of each position associated with Federal computer systems. This policy applies to positions in the competitive service occupied by Federal civilian employees. Departments and agencies may wish to adopt similar policies for any other personnel involved with, or having access to data in, Federal computer systems.

A-2. CRITERIA FOR DESIGNATING POSITIONS

Three categories have been established for designating computer and computer-related positions—ADP-I, ADP-II, and ADP-III. Specific criteria for assigning positions to one of these categories is as follows:

Category	*Criteria*
ADP-I	—Responsibility for the development and administration of agency computer security programs, and also including direction and control of risk analysis and/or threat assessment. —Significant involvement in life-critical or mission-critical systems. —Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain. —Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater, or (2) lessor amounts if the activities of the individual are not subject to technical review by higher authority in the ADP-1 category to insure the integrity of the system. —Positions involving *major* responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software. —Other positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.
ADP-II	—Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADP-I category, to insure the integrity of the system. This category includes, but is not limited to: (1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts; (2) accounting, disbursement,

Category	Criteria
	or authorization for disbursement from systems of dollar amounts less than $10 million per year. —Other positions as designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP–I positions.
ADP–III	—All other positions involved in Federal computer activities.

A–3. GUIDELINES FOR APPLYING CRITERIA TO SPECIFIC POSITIONS

In determining category levels for Federal computer positions, agency heads should consider not only the specific requirements of the position, but also the relationship of those requirements to the informational system that the position services. For example, information that is not in itself highly sensitive may in combination with similar, low sensitive data produce a highly sensitive system. A position, which involves limited access to and use of selected systems data for specific purposes during limited periods of time in a controlled situation, may be considered for a lower ADP category. Such positions might have less potential for harm than a position associated with the system's design, operation or maintenance involving access to or control of large amounts of data in the system which, in combination, may be extremely critical to life or mission.

Application of the criteria for designating category levels of individual positions normally does not fit a precise formula. A determination must be made on the basis of judgment, considering numerous factors, including, but not necessarily limited to:

—the degree of supervision or review afforded the occupant of the position;
—the extent of security and protective measures in effect;
—the nature of the data being processed;
—the degree to which the data being processed is accessible by the individual through outside terminals;
—the extent to which responsibility for violations or attempted violations of computer systems security can be established;
—the extent to which the activities associated with the position are performed in isolation from concurrent processes; and
—the degree of accessibility to other data in a system through intrusion by telecommunications or time sharing.

Based upon these and other considerations, agencies should define determinants such as *significant involvement*, *grave damage*, and *significant personal gain* in terms of the individual agency mission and the relative risks associated with the particular system or systems involved. On a continuing basis, an assessment of all category designations should be made to identify any changes in the data available or the duties and responsibilities of the position that would cause the position to be placed in a higher or lower category level.

A–4. SCREENING PERSONS FOR ASSIGNMENT TO ADP–I, ADP–II, AND ADP–III POSITIONS

Heads of agencies are responsible for developing criteria for screening persons for assignment to ADP–I, ADP–II, and ADP–III positions. The OPM's suitability guidelines in Federal Personnel Manual Supplement 731–1 and the guidelines in Executive Order 10450 may be used in developing this criteria. Agencies should also consider any other factors which have a bearing on the person's trustworthiness. Individual agency criteria for Federal civilian competitive service positions may also be used for any other personnel associated with Federal computer systems.

APPENDIX D

COMPUTER PROGRAM DOCUMENTATION

COMPUTER PROGRAM DOCUMENTATION

Opinions vary on what constitutes adequate and complete documentation of operational computer programs. It is generally agreed, however, that at least four categories of documentation are required if long and complex programs are to be significantly changed or subjected to other scrutiny.

The four categories are system flowcharts, detailed program flowcharts, source programs, and computer runsheets. Still other categories of documentation may be found when the auditor embarks on an audit of documentation supporting computer programs. The documentation may be placed in 12 different categories. They are explained here to show the relationship of various forms of documentation to the four first mentioned. The auditor is cautioned, however, that each EDP installation may not place the documentation in the precise categories described here. Some of the 12 categories may have been combined, others may have been eliminated or omitted, and still others may have been added.

1. Cover Sheet. The purpose of the cover sheet is to identify the computer program by giving such information as program name, program number, purpose (a brief nontechnical description of the problem solved by the program), source language used (such as COBOL or FORTRAN), EDP configuration that the program was designed for, programmer's name, and date of the program. Even though helpful, the cover sheet is not an absolute necessity because the information it contains is usually shown elsewhere in the documentation or is easily obtained.

2. Forms Layout. The purpose of this section is to show the content of input and output documents and reports. If it is not included in the documentation, it is usually available from other sources, such as current reports and currently used input documents.

3. Definitions. The purpose of this section is to define all symbolic names used anywhere in the program documentation. Symbolic names are abbreviated terms that are used in place of longer names, terms, or titles. For example, one of the input documents in the forms layout section may show a form space and identify its contents as "TAXDED." Reference to the definitions section might show that "TAXDED" means "Tax Deduction." This section may also contain any tables or other information the programmer feels should be defined. A table might show, for example, the number of dependents in one column and the applicable tax deduction in an adjacent column.

Exhibit 11-2. (Cont.)

Like the forms layout section, the definitions may be available from other sources if they are not defined in a separate section of documentation. As an example, definitions may be recorded on system flowcharts and detailed program flowcharts (explained later) or defined in the comments contained in the source program. Of course, the symbolic names used may have an obvious or easily determinable meaning. In that case, the definitions may not be essential.

4. System Flowchart. The purpose of the system flowchart is to show the flow of work, documents, and reports in a specific data processing job. It is designed to demonstrate how the data processing job is organized from beginning to end. It is general in nature because it does not specify the detailed and specific computer steps that are necessary for a particular processing run. (This detail is a function of the detailed program flowchart described later.)

Special data processing symbols are used in a system flowchart, along with symbolic names, previously described, and English language statements to describe flow of work, documents, and reports. By referring to the system flowchart, programmers and others can find out how the overall data processing job is organized, the source of type of input records, the point at which input records are introduced into the computer for processing, the sequence of the overall processing, all resulting output — such as printed reports — and the ultimate destination of the output.

This type of information is not usually available from another source unless it can be recalled by the people who worked on the program or unless it can be reconstructed from other detailed data processing records or current practices. Reconstruction can take a great deal of time if the data processing job is a lengthy one. Besides, it is not a good practice to rely on an individual's memory, because some important details may be forgotten or the individual may leave the company.

5. Detailed Program Flowchart. Like the system flowchart, the detailed program flowchart uses special data processing symbols, symbolic names, and English language statements. Unlike the system flowchart, however, the detailed program flowchart shows a step-by-step sequence in implementing a data processing job so that it can be made operational.

It is from the detailed program flowchart that the programmer prepares the actual computer program (called a source program) to be compiled and executed by the computer. Unless the source program is simple and only a few source program steps are required, a current detailed program flowchart is a valuable tool to the programmer in making necessary changes at a later date.

Because of its extremely detailed nature, it is important that the detailed program flowchart be kept current. Otherwise, important and minute details may be forgotten and the programmer may find it difficult or impossible to make changes in the related source program when the need arises. This is particularly true if the changes are to be made by a programmer other than the one who initially prepared the detailed program flowchart and source program. For some complex source programs, the programmer may prepare several program flowcharts, each becoming progressively more detailed until one of them possesses the detail that is necessary for writing the source program. When making program changes, the detailed program flowchart is almost always used in conjunction with the source program (described on item 7).

Exhibit 11-2. (Cont.)

6. Program Description. This section describes how the logic of the source program was developed, using the higher-level language (such as COBOL or FORTRAN) and the computer. It is a detailed flowchart in prose form. Sometimes, because COBOL is near to English, this section is not prepared for source programs written in COBOL. If it is not prepared, the same information is almost always available from the detailed program flowchart or the source program, except without the detailed and sometimes lengthy prose statements which explain why specific procedures were followed.

7. Source Program. This section contains the actual program as it is written in such higher-level languages as COBOL or FORTRAN. By comparing the detailed program flowchart with the actual source program, the programmer or others can trace each step of the computer through to a final conclusion. In reviewing and making changes in the programs, the programmer must generally refer to the source program to determine precisely how the higher-level language statements were used before the current review and change became necessary.

The detailed program flowchart is useful in determining the purpose of specific source program statements. Some EDP installations may also follow the practice of requiring programmers to include English language comments in the source program to briefly explain the purpose of each program step. Such comments are useful and, together with the detailed program flowchart, can provide a clear audit trail that shows the step-by-step procedure that was followed in developing the source program.

Sometimes, English language comments in the source program are sufficient to permit an accurate review of or change in the computer program. This, of course, depends upon the extent and clarity of the English language comments, the length and complexity of the source program, and the extent of the required review or program changes.

If a current copy of the source program is not formally kept as documentation, it can usually be obtained from punched cards that were used to introduce the source program into the computer or from other storage devices, such as magnetic tape, that may be used to hold the information.

8. List of Test Data. This section identifies the test data used by the programmer in testing the source program after it was written. The results are shown in the Test Report (described in item 10).

9. Sample Output. This section contains sample output resulting from the source program. Examples of output include reports and punched cards. If this information is not included in the documentation it is usually easily obtained by referring to recent output that resulted from EDP processing runs.

10. Test Report. This section explains the results that were obtained when the source program was tested to determine whether it was operational. If test data and test reports are not included in the documentation, the programmer can prepare other test data to determine the current effectiveness of the source program.

11. Deck Setup. This section gives the order of the source program card deck. It is similar to the source program (see item 7), but it is not in as much detail. The source program is an exact duplication of the computer program in the higher-level language. The deck setup shows the order of the related card deck, but it is usually subdivided by major category and does not outline each program step.

Exhibit 11-2. (Cont.)

This section may include such other information as requirements for peripheral equipment (magnetic tape drives, card readers, and card punchers), the time limit for the computer program when it is being executed by the computer, and special control cards needed for a successful run of the job. This information is also available from the programmer.

12. **Computer Run Sheet.** This section contains information needed by the console operator for running the computer program, such as the magnetic tapes or disks to be mounted, the names and usage of all input files, any central processing unit (CPU) console messages that may appear during the run, and any operator action to be taken as a result of these messages. This information is also usually available from retained copies of the CPU console messages from programmers responsible for maintaining the source program.

APPENDIX E

CONTINGENCY PLAN OUTLINE

Part One--Preliminary Planning

1.1 Purpose
- Reason for plan
- Objective

1.2 Scope
- Applicability of plan
  --Data center 1
  --Data center 2

1.3 Assumptions
- Events included
- Events excluded
- Priorities
- Support commitments

1.4 Responsibilities
- Plan preparation/maintenance
- Emergency chain of command
- Operations supervisor
- Shift supervisor

1.5 Strategy
- Emergency response
- Backup operations
- Recovery

1.6 Record of Changes
- Change sheet
- Plan distribution

Part Two--Preparatory Actions

2.1 People

- Complete listing of assigned personnel with address, phone number, etc.
- Emergency notification roster(s)
- Team composition

  --Recovery Team A

  --Recovery Team B

2.2 Data

- On-site inventory
- Off-site inventory

  --How/when rotated
- Critical files needed for backup site processing

2.3 Software

- System

  --On-site inventory

  --Off-site inventory

  ---How/when updated
- Applications

  --On-site inventory

  --Off-site inventory

  ---How/when rotated

2.4 Hardware

- Inventory list reflecting vendor, name, address, etc.
- Emergency acquisition agreement
- Sample order forms, etc.

2.5 Communications

- Current on-site requirements
- Requirements for backup site(s)

2.6 Supplies

- List of critical supply items with all necessary information (e.g., stock numbers for ordering)
- List of vendors who provide supplies
- List/location of supplies needed for backup site processing

2.7 Transportation

- Requirements for recovery operations/backup site(s)
- Procedures for obtaining emergency transportation

2.8 Space

- Current site requirements (lay-out of facility)
- Backup site space available, by site

2.9 Power and Environment

- Current site requirements
- Backup site requirements

2.10 Documentation

- On-site inventory
- Off-site inventory

  --How/when updated
- List/location of critical documentation needed for backup site processing

2.11 Other

- Alternate site agreements
- Contracts

2.12 Test Plans

- Plan A
- Plan B

Part Three--Action Plan

3.1 Emergency Response

- Scenario 1
- Scenario 2
- Scenario n

3.2 Backup Operations

- Scenario 1
- Scenario 2
- Scenario n

3.3 Recovery Actions

- Scenario 1
- Scenario 2
- Scenario n

NOTE: The exclusion of any item in the examples above does not imply that further entries may not be required for any facility. The purpose of the example entries is to suggest, generally, possible relevant entries for each facility's contingency plan. Most planners will undoubtedly discover that in order to provide complete coverage, further expansion of the outline will be necessary. [Ref. 32: pp. 30-32]

LIST OF REFERENCES

1. Naval Data Automation Command Conversion and Project Management Directorate, DCNO(MP&T)/NAVCOMPT Brand-X Site Study, 15 February 1979.

2. Naval Data Automation Command Conversion and Project Management Department, PERSPAY Project Economic Analysis, December 1979.

3. Ninety-third Congress, S.3418, Public Law 93-579, "Privacy Act of 1974," December 31, 1974.

4. OPNAV Instruction 5239.1A, Department of the Navy Automatic Data Processing Security Program, August 3, 1982.

5. Federal Information Processing Standards Publication 65, Guideline for Automatic Data Processing Risk Analysis, August 1, 1979.

6. Federal Information Processing Standards Publication 41, Computer Security Guidelines for Implementing the Privacy Act of 1974, 30 May 1975.

7. Sawyer, Lawrence B., The Practice of Modern Internal Auditing, The Institute of Internal Auditors, Inc., 1981.

8. Parker, Donn B., Crime by Computer, Charles Scribner's Sons, New York, 1976.

9. Browne, Peter S., Security Checklist of Computer Center Self-Audits, American Federation of Information Processing Societies, 1979.

10. Federal Information Processing Standards Publication 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, June 1974.

11. Federal Information Processing Standards Publication 48, Evaluation of Techniques for Automated Personal Identification, April 1, 1977.

12. Federal Information Processing Standards Publication 83, Guideline on User Authentication Techniques for Computer Network Access Control, September 29, 1980.

13. RP-1, Standard Practice for the Fire Protection of Essential Electronic Equipment Operations, National Fire Prevention and Control Administration, U.S. Department of Commerce, August, 1978.

14. NAVFAC DM-8, Design Manual: Fire Protection Engineering, Naval Facilities Engineering Command, September, 1973.

15. Carroll, John M., Computer Security, Security World Publishing Company, Inc., 1977.

16. Basic Installment 245, Federal Personnel Manual (with changes), United States Civil Service Commission, October 27, 1977.

17. International Business Machines Corporation Manual G520-2169-0, The Considerations of Data Security in a Computer Environment, July, 1970.

18. International Business Machines Corporation Manual G320-5649-1, Data Security Controls and Procedures--A Philosophy for DP Installations, March, 1977.

19. Patrick, R. L., AFIPS System Review Manual on Security, American Federation of Information Processing Societies, Inc., Montvale, New Jersey, 1975.

20. Wilkins, Barry J., The Internal Auditors Information Security Handbook, The Institute of Internal Auditors, Inc., 1979.

21. Federal Information Processing Standards Publication 39, Glossary for Computer Systems Security, February 15, 1976.

22. Enger, Normal L., and Howerton, Paul W., Computer Security: A Management Audit Approach, AMACOM, 1980.

23. Arens, Alvan A., and Loebbecke, James K., Auditing: An Integrated Approach, Prentice-Hall, Inc., 1980.

24. Systems Auditability and Control Study, Data Processing Control Practices Report, Stanford Research Institute, Altamonte Springs, Florida: The Institute of Internal Auditors, Inc., January, 1981.

25. International Business Machine Corporations Manual GF20-0006-1, IBM Systems Management: Management Controls for Data Processing, April, 1976.

26. NAVCOMPT Instruction 7000.36, Standard Criteria for Internal ADP Control of Financial Management Systems, Comptroller of the Navy, February 4, 1975.

27. Mair, William E., Wood, D. R., and Davis, K. W., Computer Control and Audit, Altamonte Springs, Florida: The Institute of Internal Auditors, Inc., 1976.

28. NBS Special Publication 500-33, Considerations in the Selection of Security Measures for Automatic Data Processing Systems, National Bureau of Standards, U.S. Department of Commerce, June 1978.

29. SECNAVINST 5211.5C, Personal Privacy and Rights of Individuals Regarding Records Pertaining to Themselves, 4 December 1981.

30. OPNAVINST 5510.1F, Department of the Navy Information Security Program Regulation, 29 September 1978.

31. Shaw, James K., Executive Guide to ADP Contingency Planning, July, 1981.

32. Federal Information Processing Standards Publication 87, Guidelines for ADP Contingency Planning, March 27, 1981.

33. SECNAVINST 5370.2G, Standard of Conduct, August 4, 1977.

34. SECNAVINST 5520.3, Criminal and Security Investigations and Related Activities Within the Department of the Navy, July 16, 1975.

35. SECNAVINST 5500.40, Reporting of Missing, Lost, Stolen or Recovered Government Property, April 26, 1979.

36. Myers, Philip A., Subversion--The Neglected Aspect of Computer Security, Master's Thesis, Naval Postgraduate School, Monterey, June, 1980.

37. Marine Corps Order P5510.14, Marine Corps Automatic Data Processing (ADP) Security Manual, January 2, 1981.

38. Department of Defense (DOD) Computer Security Center, Trusted Computer System Evaluation Criteria, presented at the Fifth DOD Computer Security Initiative Seminar, May 24, 1982.

39. Comptroller General of the United States Report LCD-78-123, Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data, January 23, 1979.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93940	2
3.	Department Chairman, Code 54 Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
4.	Professor Dan C. Boger, Code 54Bk Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
5.	Professor Norman F. Schneidewind, Code 54Ss Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
6.	Navy Finance Center, Code 52 Director Data Processing Department Anthony J. Celebrezze Building Cleveland, Ohio 44199	4
7.	Commandant of the Marine Corps Headquarters, United States Marine Corps Code MMOA-3 Washington, D.C. 20308 (ATTN: Major Manning)	1
8.	Lt. Col. J. F. Mullane, Jr., USMC Code 0309 Naval Postgraduate School Monterey, California 93940	1
9.	LCDR E. Hodnett, SC, USN 1123 Priscilla Lane Alexandria, Virginia 22308	2

10. Capt. Daniel E. Barber, USMC 2
2416 - 44th Street
Moline, Illinois 61265

END

FILMED

5-83

DTIC